# INFORMATION THEORETIC APPROACH IN DETECTION AND SECURITY CODES

A Dissertation
Presented to
The Academic Faculty

By

Jiaxi Xiao

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
in
Electrical and Computer Engineering

School of Electrical and Computer Engineering
Georgia Institute of Technology
May 2012

# INFORMATION THEORETIC APPROACH IN DETECTION AND SECURITY CODES

Approved by:


Dr. Steven W. McLaughlin, Advisor
*Professor, School of Electrical and Computer Engineering*
*Georgia Institute of Technology*

Dr. John R. Barry
*Professor, School of Electrical and Computer Engineering*
*Georgia Institute of Technology*

Dr. Xiaoli Ma
*Professor, School of Electrical and Computer Engineering*
*Georgia Institute of Technology*

Dr. Erik I. Verriest
*Professor, School of Electrical and Computer Engineering*
*Georgia Institute of Technology*

Dr. Geoffrey Ye Li
*Professor, School of Electrical and Computer Engineering*
*Georgia Institute of Technology*

Dr. Prasad Tetali
*Professor, School of Mathematics and School of Computer Science*
*Georgia Institute of Technology*



Date Approved: February 22, 2012

*To Zezhi Che and Chuanfu Xiao– my parents.*

# ACKNOWLEDGMENTS

I am heartily thankful to my Ph.D. advisor, Dr. Steven McLaughlin, for all the hope, encouragement and support he has put on me during all my graduate years in Georgia Tech. He has always encouraged and stayed with me in the path of research. He has enlightened me through his wide knowledge of Information and Coding Theory and his deep intuitions about where it should go and what is necessary to get there. I appreciate his support and help for both my professional and personal growth. Without his supports and guidance, I could not have gone this far.

I am also grateful to Dr. Xiaoli Ma, my Ph.D. co-advisor. I have benefited a lot from her impressive insights in research. She also helped me improve my academic writing and oral presentation significantly. I would like to thank her for her support, encouragement, and invaluable advice during my last two years' Ph.D. study.

I would like to thank Professor John R. Barry, Professor Ye Li, Professor Erik I. Verriest, and Professor Prasad Tetali for serving in my dissertation committee. Their broad perspectives and suggestions helped me a lot in refining this dissertation.

I would also like to thank all my labmates in the Coding, Communications and Information Theory Group for inspiring discussions and help. Many thanks to Willie and his family, Shayan, Matthieu, Demijan, and Arun and all my colleagues at Centergy One building. I thank all my friends at Georgia Institute of Technology. You make this place vivid, warm, and more attractive.

I have been away from home for about six years. However, my parents always give their selfless love, support and understanding to me, which are the source of my power. Without them, I will not be here. Thank them from my deepest heart.

Finally, I would like to sincerely thank my husband. He is always positive no matter what we have met. Whenever I feel desperate and depress, he always supports and encourages me without any reservation. Thank him for his deep love to me.

# TABLE OF CONTENTS

# LIST OF FIGURES

# SUMMARY

Signal detection plays a critical role in realizing reliable transmission through communication systems. With good detectors, transmission reliability can be enhanced. Maximum a posteriori (MAP) detector is taken as the optimal detector, which gives the detection result with maximum a posteriori value. Maximum-likelihood detector (MLD) and zero-forcing detector (ZFD) are the two classical detection schemes. MLD implements the statical method, maximum-likelihood estimation, to select the signal(information) with maximum-likelihood value. ZFD inverts the frequency response of the channel. But for some particular communication systems, both MAP and ML detection usually require high computation complexity, and sometime MAP and ML detection are even not applicable. This thesis first develops a novel and practical detection algorithm for *two-dimensional* (2-D) M-ary *inter-symbol interferences* (ISI) channel where MAP and MLD cannot be realized. Next, the thesis analyzes the fundamental performance of MLD and ZFD in *multiple-input multiple-output* (MIMO) systems from information theoretic point of view. The security code design to achieve physical layer communication security and reliability over wiretap channel is also studied.

Our work starts from developing a coding and detection algorithm for localized holographic data storage system. To deal with this problem, we model the whole storage system as a communication system with 2-D ISI channel and M-ary inputs. Since there is no existing efficient detection algorithm to detect the M-ary signals over 2-D ISI channel, we propose to implementing multi-level coding technology and detect the signal stage by stage. On each stage, to reduce the computation complexity, multi-strip BCJR with Gaussian approximation equalization algorithm is developed. The proposed equalization algorithm can hugely reduce the number of states for BCJR algorithm on each single data of the whole 2-D data page, which significantly reduces the computation complexity and makes the proposed equalization algorithm applicable. With the proposed detection scheme, we

also compute the achievable information rate on each level. More over, the corresponding *low-density parity-check* (LDPC) component code is designed accordingly to achieve the achievable information rate with the proposed detection algorithm.

To numerically analyze the performance of ML and ZF detection technologies in a MIMO system, the *mutual information* (MI) is widely used as a metric. Existing results on fundamental limits of MIMO systems with ML or ZF detection are focused on the assumption of continuous signals at the receiver side and the effect of detectors has largely not been addressed. However, in practical digital communication systems, when the inputs are discrete, the continuous outputs given by the receivers have to be mapped to the alphabet of the transmitted signals, *i.e.* the final outputs should also have discrete values. In this dissertation we study the mutual information between the transmitted discrete signal and the quantized estimated signal given by maximum-likelihood or zero-forcing detector in a MIMO channel setting. To differentiate this from case of the mutual information without any assumption on the detector, we establish a new metric which is the *post-detection mutual information* (PMI). When phase-shift keying (PSK) constellations are adopted, easily computable asymptotically tight low bounds of the PMI with MLD or ZFD are derived. Furthermore, when quadrature amplitude modulation (QAM) constellations are adopted, a numerically closed form of the PMI with ZFD is provided. We show how much the mutual information is reduced by the presence of quantization of the detectors. The lower bounds provided in the dissertation tightly approach the simulation results in mid and high SNR region.

For the security problem in wiretap channel, we consider a commonly adopted wiretap model which has a noiseless main channel and a binary erasure eavesdropper's channel. LDPC codes have been applied to achieve strong secrecy over such wiretap channel setting. However, it lacks design flexibility balancing on security and reliability, and cannot illustrate the fundamental tradeoffs among erasure rate, secrecy rate, and the security performance. We investigate a *random complex field code* (RCFC) design for such wiretap

channels. The design of RCFCs is systematic and flexible for any code rate. Our analysis shows that RCFC can achieve the secrecy capacity as the code length goes to infinity. More strikingly, the presented design is the first one which provides a platform to tradeoff secrecy performance with the erasure rate of the eavesdropper's channel and the secrecy rate.

# CHAPTER 1

# INTRODUCTION

## 1.1 Motivation

A communication system can be roughly decomposed of transmitters, communication channel, and detectors. The function of the detector is to recover the transmitted signal(information) based on the received signal(information). Detection is one of the key components of various communication systems. From wireless communication to data storage system, detection plays a critical role. Different communication systems have different requirements on detection. For example, in data storage system, the detection scheme should minimize the detection error rates. However, in wireless communication system, because of the existence of security issue, the detection scheme design at the legitimate receiver pursues to achieve arbitrary small error rate, while at the same time, the whole system should maximize the detection errors of the eavesdroppers' detection.

How to design detection scheme has become a hot research topic in communication research field. Maximum a posteriori (MAP) detector [1–3] is taken as the optimal detector, which gives the detection result with maximum a posteriori value. However, MAP detection usually requires high computation complexity, and sometime MAP detection is even not applicable. Maximum-likelihood detector (MLD) [4–6] and zero-forcing detector (ZFD) [7] are the two classical detection schemes. MLD implements the statical method, maximum-likelihood estimation, to select the signal(information) with maximum-likelihood value. ZFD inverts the frequency response of the channel. However, how to design the detection scheme with "good" performance and tolerant computation complexity for some particular communication systems is still a hard problem. One of such examples is holographic data storage system, which is one of next-generation storage techniques. The communication channel of holographic data storage system can be modeled as a *two-dimensional* (2-D) *intersymbol-interference* (ISI) channel. If using MLD, unacceptable

computation complexity is required. While ZFD incurs large error detection rate. To detect the stored data information in holographic data storage system, a novel and computation efficient detection scheme needs to be investigated. Meanwhile, the performance of the designed detection scheme should be quantified. Furthermore, the corresponding coding and decoding scheme needs to be developed to implement holographic data storage system.

Even for the classical and popular detection schemes like MLD and ZFD, what the limits of these detection schemes are from information theoretic point of view is still an unanswered question. One example is a *multi-input multi-output* (MIMO) system with a *maximum-likelihood detector* (MLD) or *zero-forcing detector* (ZFD). By taking advantage of the spatial diversity in wireless communications or data storage systems, multi-input and multi-output (MIMO) systems (which also represent multi-transmitter multi-receiver systems) offer significant improvement on reliable data rates compared with single-input single-output (SISO) systems [8–11]. One of the important parameters to quantify the performance of MIMO systems is mutual information (MI). To maximize MI, there are two categories of methodologies. The first category assumes channel feedback, partial feedback or finite rate feedback is somehow known at the transmitter. Under such assumptions, optimality of beamforming is deeply studied to maximize the MI of MIMO channels (see *e.g.* [12–19]). The second category assumes no channel state information at the transmitter. Under such an assumption, it is not possible to apply beamforming technology at the transmitter. Instead, continuous inputs signal without beamforming is used. At the receiver side, zero-forcing (ZF) [20–22] and maximum-likelihood (ML) [23–25] receivers are commonly adopted because they represent the extremes of the receivers in forms of performance and complexity [26, 27]. Some related previous work has been done under such assumptions. Specifically, Ma and Zhang provide the MI between the continuous transmitted signals and the continuous received signals given by ML or ZF receiver [28]. Furthermore, the underlying factor which determines the difference of MI with the two receivers is proven to be the orthogonal deficiency (*od*) of the channel matrix [28]. Most of the methods referred above

deal with continuous signals at both the transmitter and the receiver. Actually, when there is no channel information known at the transmitter, the discrete independent and identically distributed (*i.i.d.*) input symbols are of more interest from both the theoretical and practical point of view. Obviously, the discrete input signals will reduce the MI compared with the MI with continuous input signals. Some research work discussed the MI with discrete input signals. In the related work [29, 30], the MI between the discrete transmitted signal and the continuous received signal (no quantization) given by ML or ZF receiver is discussed.

It should be noted that both ML and ZF receivers considered in the existing references [20–24, 28, 29] produce continuous values. In other words, the MI discussed in the previous work is the one between the inputs and continuous outputs given by ML or ZF receiver. However, in practical digital communication systems, when the inputs are discrete the continuous outputs given by the receivers have to be mapped to the alphabet of the transmitted signals, *i.e.* the final outputs should also have discrete values. We refer to the ML (ZF) receiver with the hard mapping step as the ML (ZF) detector and call the hard outputs given by detectors as the detected signals. The hard detection step has not been considered before in the related work. Thus, we ask an important yet unanswered question: *what is the maximum information rate that can be transmitted reliably in MIMO systems when both detectors and discrete inputs are considered?*

Before answering the question, let us first explore the meaning of the question. Consider a widely used MIMO system with receivers and error-control coding. The ML or ZF receiver computes the log-likelihood ratio (LLR) of each bit of the transmitted symbols based on the raw resulting outputs and the channel response. The LLRs are transferred to the decoder as the priori information for decoding. Next the decoders compute the LLR of each bit based on the priori information provided by the receiver. Finally the hard decoded bits are determined via the LLR given by the decoders. When we design the error control codes, we need to ask what the code rates are we should use to design the codes. Obviously, the highest code rates should be the ultimate achievable information rates of

the systems. From Shannon's theorem we know that the ultimate achievable information rates of a communication system should be the MI between the inputs and outputs of that system without code gains. For MIMO systems with ML or ZF receiver, since the final hard decoding step of the decoder should be taken into account, the ultimate achievable code rates of the system are not the MI between the discrete inputs and the continuous outputs given by the receivers any more [29]. Instead, the ultimate achievable code rates of the MIMO systems with ML or ZF receiver should be equivalent to the MI between the discrete inputs and the discrete outputs of the MIMO systems with ML detector (MLD) or ZF detector (ZFD), respectively. It will be shown that the answer to the question raised here is the answer to what highest code rates can be applied in MIMO systems with a receiver. Part research work of the thesis focuses on the MI of the discrete MIMO channels with two widely adopted detectors: MLD and ZFD, which represent the extremes of the detectors in terms of performance and complexity. To differentiate from the MI without the hard mapping step, we refer to the one with hard mapping as *post-detection mutual information* (PMI). Since the hard mapping step in the detector is irreversible, we expect that the PMI is reduced compared to the MI without hard mapping. Fundamental research work is desired to carry out to find out the value of PMIs.

Another detection problem discussed in the dissertation is the security code design in communication system. More specifically, the dissertation investigates a new coding scheme for wiretap channel [31]. Wiretap channel has caught a lot of attention recently in secured communications. A commonly adopted wiretap model is that the main channel is noiseless and the eavesdropper's channel is binary erasure channel (BEC). LDPC codes have been applied to achieve strong secrecy [32]. However, it lacks design flexibility balancing on security and reliability, and cannot illustrate the fundamental tradeoffs among erasure rate, secrecy rate, and the security performance. A more flexible and easy designed security code is highly required to be investigated.

## 1.2 Our Approaches and Thesis Outline

The major goal of this research is to investigate novel signal detection and coding algorithms to improve the performance of a communication system. In particular, we consider three communication systems. The first one is *localized holographic data storage* (LHDS) system. The second one is *multiple-input multiple-output* (MIMO) system with a *maximum-likelihood detector* (MLD) or *zero-forcing detector* (ZFD). The last one is the security problem in wiretap channel.

For LHDS system, we model the channel of the system as a 2-D ISI channel with M-ary inputs, which is a more general communication channel. We adopt multi-level coding and multi-stage decoding techniques to encode the inputs and decode the outputs, respectively. However, there is no existing algorithms to equalize M-ary 2-D ISI channel. To efficiently detect the recorded information, we propose Gaussian-approximated multi-stage multi-strip BCJR equalization algorithm, which equalizes the channel stage by stage. To begin with the stage with the highest signal power level, the BCJR algorithm is used to equalize each level by averaging the interference of the undecoded levels. Both the hard and soft decisions are passed to the next stages. The detection scheme hugely reduces the complexity of full-branch BCJR on the entire received page of data and makes the detection algorithm applicable. To design the corresponding encoding scheme for the system, the achievable information rate achieved by the proposed equalization algorithm is calculated level by level via Monte Carlo simulation. Then based on the achievable information rate on each level, the corresponding semi-algebraic LDPC component code is designed. The overall performance of the coding and decoding algorithm is examined by the decoding error rate.

To find out the end-to-end mutual information between the discrete inputs and discrete outputs in a MIMO system with MLD or ZFD, we propose a new metric, *i.e., post-detection mutual information* (PMI), which describes the ultimate achievable information rate of MIMO system with MLD or ZFD. We first establish the analytical expression of

the PMI with MLD and ZFD. We observe that there is no closed form for the PMI with MLD or ZFD. However, when *phase-shift keying* (PSK) symbols are employed, we present an asymptotically tight lower bound of the PMI with MLD or ZFD. The lower bounds are easily computed which allows us to evaluate the ultimate achievable information rates for MIMO systems with detectors. Furthermore, when *quadrature amplitude modulation* (QAM) symbols are employed, we provide a simple numerical method to compute the PMI with ZFD which is shown to exactly match the simulation results. Since the hard mapping step in the detector is irreversible, we expect that the PMI is reduced compared to the MI without hard mapping. The conclusion is confirmed by both the simulation and the theoretic results. Consequently, the ultimate achievable PMI rates that can be transmitted through the MIMO channels with MLD or ZFD serve as more practical benchmarks for transmissions.

Wyner and later Csiszár and Körner prove that when the secrecy rate is below the secrecy capacity, there should exist channel codes, which can guarantee both robustness to transmission errors to the legitimate receiver and a prescribed degree of data confidentiality for the eavesdropper. Hence the wiretap channel setup can be applied in wireless communications to achieve the security in physical layer. A fundamental and well adopted wiretap channel model is that the main channel is noiseless and the eavesdroppers' channel is binary erasure channel (BEC). LDPC codes have been applied to achieve secrecy capacity of such wiretap channels. However, it lacks design flexibility and cannot illustrate the fundamental tradeoffs among the secrecy rate, erasure rate, and the secrecy performance. We propose a random complex field code (RCFC) design for such wiretap channels [33]. In RCFC, we have three kinds of sybmbols, *i.e.,* the information symbols, the check symbols, and the random symbols, all of which are QAM symbols. We mix them together by using linear complex encoder such that the information symbols can be hidden among the other symbols. The design of RCFCs is systematic and flexible for any code rate. Our analysis shows that RCFC can achieve the secrecy capacity as the code length goes to infinity. More

strikingly, the proposed design is the first one which provides a platform to tradeoff secrecy performance with the erasure rate of the eavesdropper's channel and the secrecy rate.

This dissertation is organized as follows. Chapter 2 introduces concepts and fundamental results of the above problems, summarizes the state of the art, and sets the notation used in subsequent chapters. Our main discussion and results are contained in Chapters 3-5. Specifically, Chapter 3 proposes the coding and equalization for M-ary ISI channel. Chapter 4 presents the meaning and bounds for the PMI of a MIMO system with MLD or ZFD. Chapter 5 introduces RCFC codes and analyzes its' performance in wiretap channel. Chapter 6 summarizes our conclusions and points to areas for future research.

# CHAPTER 2

# FUNDAMENTALS

In this chapter the following fundamental results are summarized:

- Introduction on holographic data storage system, the corresponding system model, and the existing detection schemes.
- Fundamental results on MLD and ZFD from information theoretic point of view.
- Information theoretic security over wiretap channel

## 2.1 Holographic Data Storage System

This section introduces the holographic data storage system and its' system models. Moreover, some related detection schemes are reviewed. As it will be shown, to efficiently detect the inputs of the system, a new detection algorithm is required to be developed.

Holographic data storage is an alternative approach for next-generation memory schemes that is expected to exceed the fundamental limits of conventional 2-D surface storage technologies like magnetic hard disk drives, optical disks, and semiconductor memories. Instead of recording the data on the surface, holographic storage stores the information in three dimensions [34]. As shown in Figure 2.1, in a holographic storage system, 2-D pixelated patterns with data page information are imposed by a *spatial light modulator* (SLM) and are recorded as holograms. Each data page is later retrieved by reading its associated hologram, which reconstructs the image of the entire input pattern. The reconstructed image of the stored data page is captured by a camera that is typically a *charge-coupled device* (CCD) camera.

Under the two following assumptions:

1. the center of each input pixel at the SLM is exactly imaged onto the center of its corresponding pixel at the CCD, and

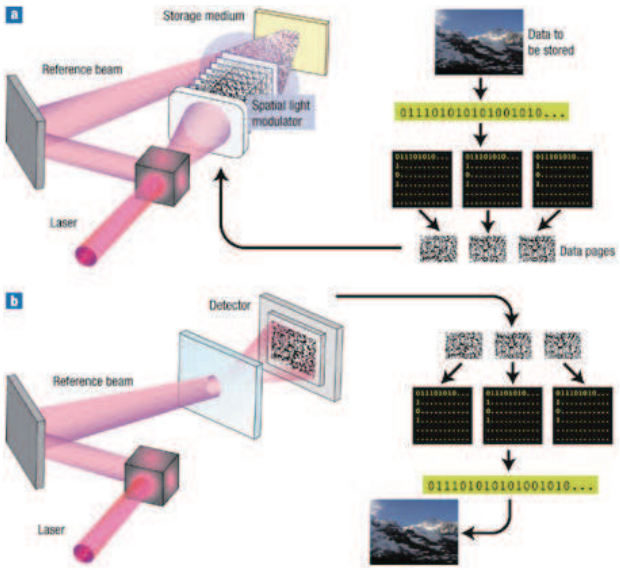
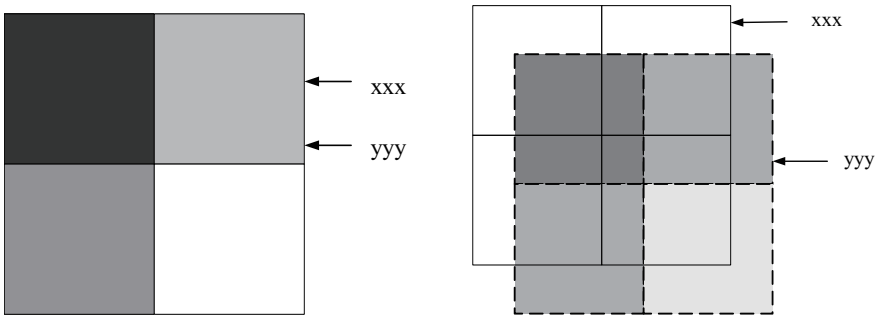



**Figure 2.1. Working mechanism of holographic data storage system.**

2. the image is confined within the CCD pixel area,

the whole system can be modeled as 2-D communication through parallel noisy channels, as shown in Figure 2.2(a).




(a) No pixel misregistration. (b) With pixel misregistration

**Figure 2.2. Images on SLM and CCD**

However, to fulfill these assumptions becomes quite challenging when high-density 2-D patterns are employed. Specifically, when high-density 2-D patterns are employed, the unlimited bandwidth of the optical system and the pixel misregistration in the two dimensions $x$ and $y$ over the recording data page produced by the magnification error, misalignment, and optical distortion bring the interference between pixels, as shown in Figure 2.2(b).

Thus, the intensity of the pixel image on CCD is simultaneously determined by the intensity of the corresponding pixel on SLM, the intensities of its neighbor pixels, and the post-detected noise. Hence when the pixels of the 2-D input page are either dark or bright, the page-oriented data recording and retrieving process is generally modeled as the communication through a noisy 2-D ISI channel with 2-D pages of binary inputs [35, 36]. However, most recently, some new holographic recording techniques such as *localized holographic* (LH) recording are currently being developed very quickly [37]. Compared with the conventional angular multiplexed holographic recording, the LH recording scheme provides much higher diffraction efficiency for each data page during the readout, which results in much larger *signal-to-noise ratio* (SNR) [38]. The excess of the SNR enables M-ary data coding, i.e., multiple gray levels of the pixel intensity [39]. Compared to the conventional angular multiplexed holographic recording system, fewer data pages can be recorded in the LH system, hence M-ary data coding can achieve higher coding gains to compensate the capacity loss and make the capacity of the LH recording comparable to or potentially larger than the traditional angular multiplexing holographic recording. The LH recording with M-ary inputs can be accordingly modeled by

$$y(i,j) = \sum_{p=0}^{L_y} \sum_{q=0}^{L_x} h(p,q)x(i-p, j-q) + n(i,j), \tag{2.1}$$

where $x(i,j) \in \{-M+1, \ -M+3, \cdots, M-3, \ M-1\}$ is M-ary input and $y(i,j)$ is the corresponding output. $n(i,j)$ is the post-detected noise, which is assumed to be Gaussian noise with zero mean and with covariance $\sigma^2 \boldsymbol{I}_{n\times n}$. $h(p,q)$ is the discrete channel response with finite span. $L_x$ and $L_y$ represent, respectively, the interference depth of the channel in the $x$ and $y$ directions. Define the *signal-to-noise ratio* (SNR) of the system as

$$SNR = \frac{E_s}{N_0} = \frac{E\left[|x(i,j)|^2\right]}{\sigma^2}. \tag{2.2}$$

When the channel is with *one-dimensional* (1-D) ISI, the *Bahl-Cocke-Jelinek-Raviv* (BCJR) algorithm [40] is well proven to be efficient to equalize the channel [41, 42]. But,

when the channel is with 2-D ISI, there is no direct extension of the BCJR algorithm to the 2-D case. Moreover, even for a 1-D ISI channel, if the inputs are M-ary, the number of states of the trellis diagram is increased from $2^L$ to $M^L$ ($L$ is the interference length), which increases the computation complexity significantly. For a 2-D ISI channel with binary inputs, the iterative multistrip BCJR algorithm is proposed to be a sub-optimal way to equalize the channel [43]. By applying the iterative multistrip BCJR algorithm on a limited region of the whole page, the upper and lower bounds of the symmetric information rates for 2-D ISI channels with binary inputs are calculated [44]. Unfortunately, when the inputs are M-ary, the computation of the iterative multistrip BCJR is still too complex to be affordable. How to efficiently equalize the 2-D ISI channels with M-ary inputs with affordable complexity is a question not previously answered.

Of particular interest to this disertation is to design an efficient detection algorithm and coding scheme for a LH data recording system and to evaluate the performance of the proposed detection from the information theoretic point of view. As will be shown, by employing multilevel coding, multistage decoding, and averaging the interference of the undecoded levels, the detection algorithm and coding scheme proposed in this dissertation reduces the complexity of full-branch BCJR and makes the whole design applicable [45]. More generally, the designed detection algorithm can be implemented to detection for 2-D ISI channel with M-ary inputs.

## 2.2 MIMO System with MLD or ZFD

In this section, we first present the general MIMO channel model and give the definitions for MLD and ZFD considered in the dissertation. Then we review some existing results and conclusions about the information rates of MIMO channels. Based on these results the goal of our research is presented.

### 2.2.1 System Model of MIMO with MLD or ZFD

We focus on the discrete-time MIMO channel with $M$ transmitters and $N$ receivers. The transmission over the channel can be described by

$$\boldsymbol{y} = \boldsymbol{H}\boldsymbol{s} + \boldsymbol{\omega}, \tag{2.3}$$

where $\boldsymbol{y}$ is the $N \times 1$ received vector, $\boldsymbol{s}$ is the $M \times 1$ transmitted signal, $\boldsymbol{H}$ is an $N \times M$ complex Gaussian distributed channel matrix, and $\boldsymbol{\omega}$ is *i.i.d.* zero-mean complex Gaussian noise with covariance matrix $E[\boldsymbol{\omega}\boldsymbol{\omega}^{\mathcal{H}}] = \sigma_{\omega}^2 \boldsymbol{I}_N$. In the following we focus on the case $M = N$.

Let $s_k$ be the $k$th element of $\boldsymbol{s}$ which is drawn from complex QAM or PSK constellation $\mathcal{S}$ with equal probability. The signal-to-noise ratio (SNR) of the channel is defined as

$$SNR = \frac{E_s}{N_0}, \tag{2.4}$$

where $E_s = E[|s_k|^2]$ and $N_0 = 2\sigma_{\omega}^2$.

Note that for different channel models, $\boldsymbol{H}$ has different structures. For quasi-static fading channels, the entries of $\boldsymbol{H}$ are modeled as zero mean, circularly symmetric, complex Gaussian random variables. For data recording channels, $\boldsymbol{H}$ is modeled as a constant matrix, the entries of which represent the channel responses. Thus, the model described in (2.3) is general enough to represent most linear channels.

We define the detection process including equalization of the received vector $\boldsymbol{y}$ and the hard mapping of the equalized vector to finite constellation.

#### *2.2.1.1 ZFD description*

The structure of ZFD is shown in Fig. 2.3. The first step is equalizing the received vector $\boldsymbol{y}$ which is given as

$$\boldsymbol{x} = \boldsymbol{H}^{\dagger}\boldsymbol{y} = \boldsymbol{s} + \boldsymbol{\eta}, \tag{2.5}$$

where $\boldsymbol{H}^{\dagger} = (\boldsymbol{H}^{\mathcal{H}}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathcal{H}}$, $\boldsymbol{x}$ is the equalized vector given $\boldsymbol{y}$, and $\boldsymbol{\eta} = \boldsymbol{H}^{\dagger}\boldsymbol{\omega}$. The covariance matrix of the equalized noise $\boldsymbol{\eta}$ is

$$\boldsymbol{W} = E[\boldsymbol{\eta}\boldsymbol{\eta}^{\mathcal{H}}] = \boldsymbol{H}^{\dagger}(\boldsymbol{H}^{\dagger})^{\mathcal{H}} E[\boldsymbol{\omega}\boldsymbol{\omega}^{\mathcal{H}}] = \sigma_{\omega}^2 (\boldsymbol{H}^{\mathcal{H}}\boldsymbol{H})^{-1}. \tag{2.6}$$

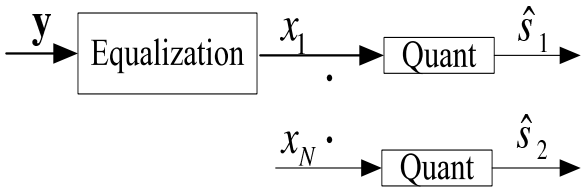



**Figure 2.3. The scheme of ZFD.**

As shown in (2.6), the equalization introduces the correlation among the noise entries. However, in the hard mapping step of the ZFD, the correlations between the noise entries are not considered. The ZFD maps $\boldsymbol{x}$ symbol by symbol. For example, the $k$th entry of $\boldsymbol{x}$ denoted as $x_k$ is mapped to the alphabet $\mathcal{S}$ as

$$\hat{s}_k = \mathfrak{Q}_s(x_k) = \underset{\tilde{s}_k \in \mathcal{S}}{\arg\min} \|x_k - \tilde{s}_k\|^2, \ k = 1, \cdots, N, \tag{2.7}$$

where $\mathfrak{Q}_s(\cdot)$ represents the hard mapping operation of ZFD, $\hat{s}_k$ is the $k$th detected symbol of the detected signal $\hat{\boldsymbol{s}}_{ZF}$ given by ZFD.

### 2.2.2 MLD description

MLD directly maps the received vector $\boldsymbol{y}$ to an M-dimensional space $\mathcal{S}^M$, which is given as

$$\hat{\boldsymbol{s}}_{ML} = \mathfrak{Q}_v(\boldsymbol{y}) = \underset{\tilde{\boldsymbol{s}} \in \mathcal{S}^M}{\arg\min} \|\boldsymbol{y} - \boldsymbol{H}\tilde{\boldsymbol{s}}\|^2, \tag{2.8}$$

where $\mathfrak{Q}_v(\cdot)$ represents the hard mapping operation of MLD and $\hat{\boldsymbol{s}}_{ML}$ is the final detected signal given by MLD. The hard mapping operation of MLD given in (2.8) is equivalent to quantizing the equalized vector $\boldsymbol{x}$ to $\mathcal{S}^M$. The equivalent form of (2.8) is:

$$\hat{\boldsymbol{s}}_{ML} = \mathfrak{Q}_v(\boldsymbol{x}) = \underset{\tilde{\boldsymbol{s}} \in \mathcal{S}^M}{\arg\min} (\boldsymbol{x} - \tilde{\boldsymbol{s}})^{\mathcal{H}} \boldsymbol{W}^{-1} (\boldsymbol{x} - \tilde{\boldsymbol{s}}), \tag{2.9}$$

and the structure of the equivalent MLD is shown in Fig. 2.4.

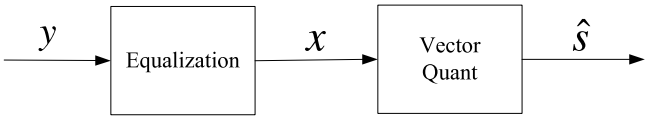



**Figure 2.4. The scheme of MLD.**

*Remark:* $\mathfrak{Q}_v(\cdot)$ and $\mathfrak{Q}_s(\cdot)$ seem similar to source quantization [46]. For example, MLD quantizes the signal vector based on the full covariance matrix of the equalized signals, which can be interpreted as vector quantizer [47, 48]. ZFD quantizes the entries of the signals one by one without considering the correlations of the entries, and thus can be interpreted as scalar quantizer [46, 49]. However, the detection is not the same as the source quantization in at least two aspects. The first one is for detectors, the quantization alphabet is pre-defined. For example, if 4-QAM is used for the transmission, the detected symbols should also be in 4-QAM constellation. The second one does not consider rate distortion nor information loss in detection, but deals more on the noise effect. Therefore, the PMI with MLD or ZFD can not be solved using source quantization theory.

### 2.2.3 Existing Results and Problem Formulation

In this section, we review some existing results and conclusions about the information rates of MIMO channels.

Several cases are discussed here. The first one is that the transmitted signal is allowed to be drawn from a continuous set and the channel matrix is known at the receiver. Under such a condition, the maximum MI with ML or ZF receiver can be achieved when the transmitted signals are complex Gaussian distributed with zero mean. Thus, the instantaneous MI with ML or ZF receiver is presented in [9, 28, 50] which are given by

$$C_{ML}(\boldsymbol{H}) = \log_2\left[\det\left(\boldsymbol{I}_M + \frac{1}{\sigma_\omega^2}\boldsymbol{H}\boldsymbol{R}_s\boldsymbol{H}^{\mathcal{H}}\right)\right], \tag{2.10}$$

and

$$C_{ZF}(\boldsymbol{H}) = \log_2\left[\det\left(\boldsymbol{I}_M + \boldsymbol{R}_\eta^{-1}\right)\right], \tag{2.11}$$

where $\boldsymbol{R}_s$ is the covariance matrix of the transmitted symbols $\boldsymbol{s}$ and

$$\boldsymbol{R}_\eta = diag[W_{1,1}, W_{2,2}, \cdots W_{M,M}], \tag{2.12}$$

with $W_{m,m}$ being the $(m,m)th$ entry of the full covariance matrix $\boldsymbol{W}$ given in (2.6). When

$\boldsymbol{R}_s = \boldsymbol{I}_M$ and the SNR is high, the difference between $C_{ML}$ and $C_{ZF}$ is approximated by [28]

$$C_{ML} - C_{ZF} \approx -\log_2\left(1 - od(\boldsymbol{H}(\boldsymbol{H}^{\mathcal{H}}\boldsymbol{H}))\right), \tag{2.13}$$

where $od(\boldsymbol{H})$ is the orthogonal deficiency of $\boldsymbol{H}$ and is defined by [28]

$$od(\boldsymbol{H}) = 1 - \frac{\det(\boldsymbol{H}^{\mathcal{H}}\boldsymbol{H})}{\prod_{m=1}^{M} \|\boldsymbol{h}_m\|^2}, \tag{2.14}$$

where $\boldsymbol{h}_m$ is the $m$-th column of $\boldsymbol{H}$.

Secondly, when the transmitted signals are discrete, *i.e.*, each symbol is drawn from a QAM or PSK constellation with equal probability, the instantaneous MI of the MIMO system with ML receiver is the MI between the discrete transmitted signal $\boldsymbol{s}$ and the continuously equalized signal $\boldsymbol{x}$ given the full covariance matrix $\boldsymbol{W}$ [29, 51]

$$\begin{aligned}
\mathcal{I}_{ML}(\boldsymbol{s};\boldsymbol{x}|\boldsymbol{W}) &= \mathcal{H}(\boldsymbol{s}) - \mathcal{H}(\boldsymbol{s}|\boldsymbol{x},\boldsymbol{W}) \\
&= \mathcal{H}(\boldsymbol{s}) + E_{\boldsymbol{s}|\boldsymbol{x},\boldsymbol{W}}\left(\log_2 p\left(\boldsymbol{s}|\boldsymbol{x},\boldsymbol{W}\right)\right) \\
&= M\log_2 q + E_{\boldsymbol{s}}\left(E_{\boldsymbol{x}|\boldsymbol{s},\boldsymbol{W}}\left(\log_2 \frac{p(\boldsymbol{x}|\boldsymbol{s},\boldsymbol{W})}{\sum_{\tilde{\boldsymbol{s}}\in\mathcal{S}^M} p(\boldsymbol{x}|\tilde{\boldsymbol{s}},\boldsymbol{W})}\right)\right),
\end{aligned} \tag{2.15}$$

where $\mathcal{H}(\cdot)$ is the entropy, $q$ is the size of the input symbol alphabet $\mathcal{S}$ and

$$p(\boldsymbol{s}|\boldsymbol{x},\boldsymbol{W}) = \frac{1}{(\pi\sigma_\omega^2)^M|\boldsymbol{W}|^{1/2}} \exp\left(-\frac{(\boldsymbol{x}-\boldsymbol{s})^{\mathcal{H}}\boldsymbol{W}^{-1}(\boldsymbol{x}-\boldsymbol{s})}{\sigma_\omega^2}\right). \tag{2.16}$$

Different from the MI with ML receiver, the MI with ZF receiver is the MI between $\boldsymbol{s}$ and $\boldsymbol{x}$ given $\boldsymbol{R}_\eta$ [29, 52]

$$\mathcal{I}_{ZF}(\boldsymbol{s};\boldsymbol{x}|\boldsymbol{R}_\eta) = M\log_2 q + E_{\boldsymbol{s}}\left(E_{\boldsymbol{x}|\boldsymbol{s},\boldsymbol{R}_\eta}\left(\log_2 \frac{p(\boldsymbol{x}|\boldsymbol{s},\boldsymbol{R}_\eta)}{\sum_{\tilde{\boldsymbol{s}}\in\mathcal{S}^M} p(\boldsymbol{x}|\tilde{\boldsymbol{s}},\boldsymbol{R}_\eta)}\right)\right), \tag{2.17}$$

where

$$p(\boldsymbol{s}|\boldsymbol{x},\boldsymbol{R}_\eta) = \frac{1}{(\pi\sigma_\omega^2)^M|\boldsymbol{R}_\eta|^{1/2}} \exp\left(-\frac{(\boldsymbol{x}-\boldsymbol{s})^{\mathcal{H}}\boldsymbol{R}_\eta^{-1}(\boldsymbol{x}-\boldsymbol{s})}{\sigma_\omega^2}\right). \tag{2.18}$$

In summary, $C_{ML}(\boldsymbol{H})$ and $C_{ZF}(\boldsymbol{H})$ given in (2.10) and (2.11) are the upper bounds of the MI of MIMO systems with ML and ZF receivers, respectively. The bounds can be achieved

only when the inputs are Gaussian continuous signals, whereas $\mathcal{I}_{ML}$ and $\mathcal{I}_{ZF}$ given in (2.15) and (2.17) are the upper bounds of the MI of the MIMO systems with discrete inputs by employing ML and ZF receivers, respectively. However, when the hard mapping step is adopted in MIMO systems, the achievable information rates become the MI between the discrete transmitted signal $\boldsymbol{s}$ and the discrete detected signal $\hat{\boldsymbol{s}}_{ML}$ in (2.9) or $\hat{\boldsymbol{s}}_{ZF}$ in (2.7). The MI between $\boldsymbol{s}$ and $\hat{\boldsymbol{s}}_{ML}$ ($\hat{\boldsymbol{s}}_{ZF}$) is referred as the PMI with MLD (ZFD) in this dissertation. The PMI with MLD or ZFD is actually the highest information rates one should apply in the system when error control codes are employed in the MIMO systems with ML or ZF receiver, respectively. All other MI rates people derived are just loose upper bounds for PMI without considering the irreversible hard mapping operation.

## 2.3 Information-Theoretic Security

Traditionally, the classical cryptographic security, which is referred to as *computational security*, is established above the physical layer. The computational security is based on the assumptions of bounded computational power of an eavesdropper, and the unproven difficulty of some particular one-way functions. For instance, in well-known cryptography RSA, the security is based on the difficulties in factoring large numbers and taking $e$-th roots modulo a composite number. However, if efficient algorithms are developed to solve the above two problems, the system will become insecure. In contrast with computational security, *information-theoretic security* model established on the physical layer, is realized by exploiting the randomness of communication channels. Different from computational security protocol, information-theoretic security protocol does not need any computational restriction on the eavesdropper. Intensive research results have shown that physical layer security can potentially, significantly strengthen the security of communication systems. Actually, the security can be provided in different layers. The physical-layer security protocol may provide more security to a communication system together with the classical computational security protocol.

To achieve secure communication via information-theoretic approach is first introduced and defined by Shannon [53]. In Shannon's classical cryptosystem, Alice wants to transmit the plaintext message $\boldsymbol{s}$ to the legitimate receiver Bob. But the eavesdropper Eve can somehow access the insecure channel. Shannon assumed that the message received by Eve is identical with the one received by Bob. To achieve the secure transmission, instead of transmitting $\boldsymbol{s}$ directly, Alice transmits the cipertext $\boldsymbol{x}$, which is obtained by Alice as a function of $\boldsymbol{s}$ and a secret key $\boldsymbol{k}$. The secrete key $\boldsymbol{k}$ is shared by Alice and Bob. Shannon proved that when $\mathcal{H}(\boldsymbol{k}) \geq \mathcal{H}(\boldsymbol{s})$, where $\mathcal{H}(\cdot)$ represents the entropy, the *perfect secrecy* can be achieved (the mutual information between $\boldsymbol{s}$ and $\boldsymbol{k}$ is zero), i.e., $\mathcal{I}(\boldsymbol{s}; \boldsymbol{x}) = 0$.

In 1975, Wyner introduced another scenario of communication with information-theoretic security [31]. In his seminal work, the wiretap channel is introduced. Generally, the secure communication over wiretap channels can be realized by two categories of methods. The first one is generating secrete keys and the other is forward coding. The secrete key generation/distribution problems in wiretap channels, which can be solved by the methodologies of key generation from correlated source outputs, have been extensively studied [54–56]. The objective of secure key distribution is for the sender Alice and the legitimate receiver Bob to achieve a common $k$-bit key about which the eavesdropper Eve's entropy is maximal. In key distribution, the key can be unknown to Alice before transmission and in most protocols, it can be achieved by some level of interactive or one-way feed-forward communication between Alice and Bob [54, 55]. Powerful tools such as common randomness, advantage distillation, and privacy amplification were developed and studied [55, 57]. Several key distribution protocols have been developed and studied for different wiretap channel scenarios. Most key agreement protocols require exchanging information by way of a parallel, error-free public channel between Alice and Bob.

In contrast to security key generation/distribution problem, the principle of the forward coding methodology is to encode $m$-bit confidential message $\boldsymbol{s}$ in $n$-bit codeword $\boldsymbol{x}$,

through which both reliable and secure communication between Alice and Bob can be realized. Theoretically, when the secrecy rate is below the secrecy capacity, there should exists a coding scheme to achieve both reliable and secure transmission simultaneously. Unfortunately, how to design the effective codes for a wiretap channel is still an open problem. The early work of forward coding and modulation schemes for wiretap channels are provided in [31] and [58]. The code construction condition presented in [31] and [58] has been extensively studied by Wei [59]. More recently, Thangaraj *et al.* shows how to design LDPC codes to achieve the secrecy capacity asymptotically for erasure wiretap channel and noiseless main channel. Recently, several authors have proved the existence of coding schemes for various generalized wiretap channel scenarios. However, as discussed earlier, it is very hard to design LDPC codes with any desired code rates. Moreover, the computation complexities for both encoding and decoding are quite high. In addition, in practical system, the requirement for security may not be as strictly as the security criteria defined in information-theoretic security problem. By scarifying some level of security, less computation complexity and more reliability can be realized. But, to our knowledge, the estimation of security performance for LDPC codes with the secrecy rate, which is beyond the secrecy capacity of the wiretap channel, are still not available.

## 2.4 Conclusion

In this chapter, we first introduce localized holographic data storage system. Based on the working mechanism of the system, we model the system as a general communication system with M-ary inputs and 2-D ISI channel. Next, we review the existing detection technologies for ISI channel. But all the existing technologies can not be applied directly to detect the M-ary 2-D ISI channel either due to the constraint of computation complexity or due to the detection error probability. A new computation-efficient detection algorithm for M-ary 2-D ISI channel needs to be investigated. Then we describe the MIMO with MLD or ZFD. By reviewing the existing results on the information rates of MIMO system with

ML receiver or ZF receive, we find that when inputs are discrete, the ultimate information achieved by MLD or ZFD is actually less than the known value. Therefore, a more practical benchmark of the information rate of MIMO with MLD or ZFD needs to be studied. Finally, we introduce the information-theoretic Security and the relevant work on how to realize information-theoretic security in wiretap channel. We also claim that a more robust code design needs to be developed.

# CHAPTER 3

# DETECTION AND CODE DESIGN FOR M-ARY 2-D ISI CHANNEL

Localized holographic data storage is an alternative approach for next-generation memory schemes that is expected to exceed the fundamental limits of conventional *two-dimensional* (2-D) surface storage technologies like magnetic hard disk drives, optical disks, and semiconductor memories. Due to the misregistration and noise, the whole system can be modeled as a communication system with M-ary inputs and 2-D ISI communication channel. As summarized in Chapter 2 the existing detection schemes can either achieve low detection error with unapplicable computation complexity, or realize computation efficiency by sacrificing detection error rate.

In this chapter, we present an computationally efficient sub-optimal detection algorithm and coding scheme for 2-D ISI channel with M-ary inputs by using multilevel coding [60–62] and multistage decoding [63–65]. The basic idea is to equalize the channel stage by stage. To begin with the stage with the highest signal power level, the multi-strip BCJR algorithm is used to equalize each level by averaging the interference of the undecoded levels. Both the hard and soft decisions are passed to the next stages. The detection scheme hugely reduces the complexity of full-branch BCJR on the entire received page of data and makes the detection algorithm applicable.

The remainder of this chapter is organized as follows. In Section 3.1, we describe the channel model and notations. In Section 3.2, we present the detection mechanism for M-ary 2-D ISI channel, which is multi-level coding and multi-stage decoding mechanism. Section 3.3 investigates the equalization algorithm at each stage, which computes the soft information that is transferred to the next stage serving as a priori information. In Section 3.4, we compute the information rate of each level achieved by the proposed detection algorithm. Section 3.5 presents the LDPC code [66–68] design to achieve the information

rate given by Section 3.4. Finally we conclude this chapter in Section 3.6.

## 3.1 Channel Model

The channel model considered in this chapter is a typical 2-D ISI channel which is given by

$$y(i,j) = \sum_{p=0}^{L_y}\sum_{q=0}^{L_x} h(p,q)x(i-p, j-q) + n(i,j), \tag{3.1}$$

where $x(i,j) \in \{-M+1,\ -M+3, \cdots, M-3,\ M-1\}$ is M-ary input and $y(i,j)$ is the corresponding output. $n(i,j)$ is the post-detected noise, which is assumed to be Gaussian noise with zero mean and with covariance $\sigma^2 \boldsymbol{I}_{n\times n}$. $h(p,q)$ is the discrete channel response with finite span. $L_x$ and $L_y$ represent, respectively, the interference depth of the channel in the $x$ and $y$ directions. Define the *signal-to-noise ratio* (SNR) of the system as

$$SNR = \frac{E_s}{N_0} = \frac{E\left[|x(i,j)|^2\right]}{\sigma^2}. \tag{3.2}$$

The problem is how to detect the M-ary input $x(i,j)$ given $y(i,j)$ and the channel response $h(p,q)$.

## 3.2 Detection Mechanism

This section introduces the detection mechanism. As it will be shown as the following, to realize M-ary inputs, a natural coding method is *multi-level coding* (MLC) scheme, which participates the information sequence into several blocks. In each block, a component encoder is used to encode the block-wise information. Using multilevel coding, on each level, we have a binary sequence. Different power is assigned to different levels. When the sequences are transmitted through the channel, accordingly, the sequence on higher level have higher SNR than the one on lower level. The resulted different SNR on different levels provide the opportunity to detect the sequences stage by stage, which is *multi-stage decoding* (MLD).

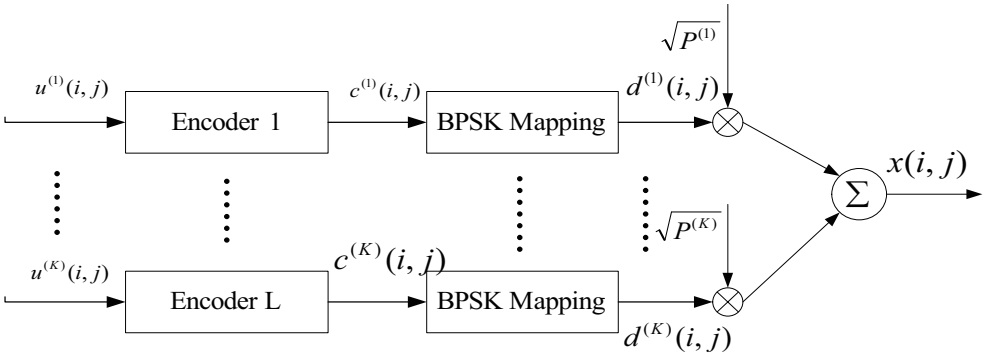



**Figure 3.1. Multilevel coding scheme**

### 3.2.1 Multilevel Coding

The MLC scheme used in the our detection algorithm is shown in Figure 3.1. The user data stream $\boldsymbol{u}$ are partitioned into $K = \log_2 M$ blocks from $\boldsymbol{u}^{(1)}$ to $\boldsymbol{u}^{(K)}$. $M$ is the number of aries of the inputs and $K$ represents the number of levels that is needed for M-ary inputs. Each symbol of $\boldsymbol{u}^{(k)}$ for $k = 1, \cdots, K$ is a binary symbol, *i.e.,* $u^{(k)}(i) \in \{0,\ 1\}$. Next, each block $\boldsymbol{u}^{(k)}$ is encoded by the corresponding binary encoder on level $k$ to $\boldsymbol{c}^{(k)}$. After getting the codeword $\boldsymbol{c}^{(k)}$ on level $k$, each bit of $\boldsymbol{c}^{(k)}$, which is denoted as $c^{(k)}(i, j)$ is mapped to BPSK signal $d^{(k)}(i, j) \in \{-1,\ 1\}$, where $(i, j)$ denotes the symbol on $(i, j)$ pixel. Now we have got $K$ encoded data block from $\boldsymbol{d}^{(1)}$ to $\boldsymbol{d}^{(K)}$. The next step is to combine them together to generate the M-ary input data stream. According to the design criteria of multilevel coding, different signal power $P^{(k)}$ is assigned to level $k$, with the largest power $P^{(K)}$ being assigned on level $K$ and the smallest power $P^{(1)}$ being assigned on level 1. Up to the step, the M-ary input data $x(i, j)$ is derived by

$$x(i, j) = \sum_{k=1}^{K} \sqrt{P^{(k)}} d^{(k)}. \tag{3.3}$$

### 3.2.2 Multistage Decoding

To decode $d^{(k)}$ via the received data page $y$, we employ *multistage decoding* (MSD) method. The multi-stage decoding mechanism implemented in the research work is illustrated in Figure 3.2. Starting from level $K = \log_2 M$, which has the highest signal power to level 1,

the input sequences on different levels are decoded stage by stage. Given the received data of the whole page $y$, the soft information about the sequence on level $K$ is fist calculated. The soft information is then passed to the decoder for level $K$ serving as a priori information. Next, the decoder for level $K$ further computes the posteriori information about the input sequence on level $K$ based on the encoding algorithm. The hard decision on $K$-th sequence is drawn based on the posteriori information given by the corresponding decoder. Till now, the input sequence on level $K$ has been hard decoded. Both the posteriori information and the hard decision for level $K$ are available now. Next stage is to decode the input sequence on level $K-1$. To decode level $k-1$, the posteriori information for level $K$ is taken as known information. Following the similar steps as decoding level $K$, both the posteriori information and the hard decision for level $K-1$ are achieved after decoding level $K-1$. Then we are ready to enter the next stage, which is decoding level $K-2$. Different from decoding level $K-1$, both the hard decision on level $K$ and the posteriori information on level $K-1$ are sent to this stage as known information. Actually, the reason why we would send the hard decision on level $K$ instead of sending the posteriori information on it to save the computation complexity. Similarly, when decoding an arbitrary level $k$, the hard decision on level $k-2$ to $K$ as well as the posteriori information on level $k-1$ are taken as known information. All the sequences on different levels can be decoded following this multistage decoding routine.

An extreme case for MSD is the input are binary sequence, thus there is only one stage. Once the stage is decoded, the whole input symbol is decoded. If the inputs are M-ary symbols, there should be $\log_2 M$ stages.

## 3.3 Equalization Algorithm

As presented in the previous section we adopt MLC and MSD as the coding and decoding scheme. Now the remained question is how to equalize the interference of the 2-D ISI channel on each decoding stage. The existing equalization algorithms for 1-D ISI channel

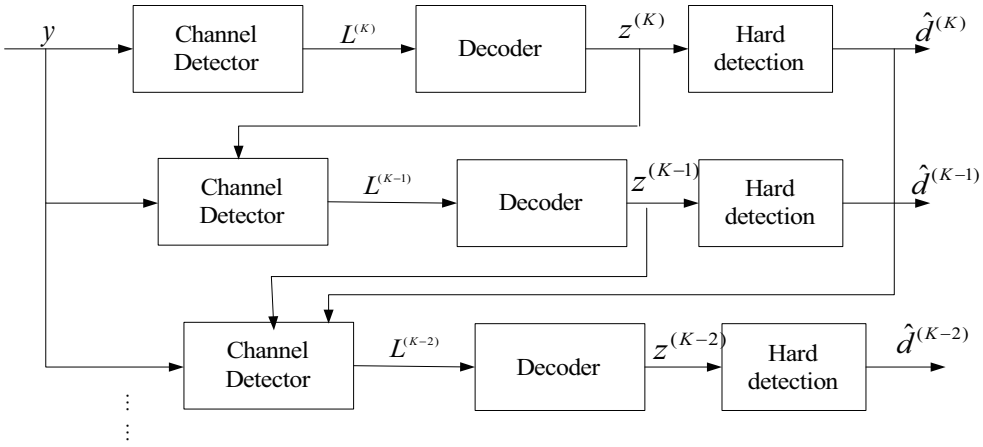



**Figure 3.2. Multistage decoding mechanism**

and 2-D ISI channel with binary inputs have been reviewed in Chapter 2. However, when the inputs are M-ary symbols, if we still use these existing technologies, the computation complexity will be hugely increased. This section proposed a new equalization algorithm which can efficiently equalize M-ary 2-D ISI channel with affordable computation complexity. The fundamental idea is employing the BCJR algorithm on each stage iteratively through the strips of the data page as in [9]. To reduce the computation complexity to an affordable level, on each stage, instead of applying the full-branch BCJR algorithm, the BCJR algorithm is only employed on reduced states by considering the bits from the undecoded levels as independently and identically distributed with equal probability. In this proposed decoding approach, the computation complexity on each binary input on each level is reduced from $2^{L_x \times L_y}$ to $M^{L_x \times L_y}$.

### 3.3.1 Multistage Multi-strip Equalization

For a *maximum a posteriori* (MAP) detection for binary 1-D ISI channel, the ultimate goal is to find out the *log a posterior probability ratio* (LAPPR) of $(i, j)$th input $x(i, j)$, which is defined by

$$LAPPR(i) = \log\left[\frac{P(x(i) = -1|\boldsymbol{y}}{P(x(i) = 1|\boldsymbol{y})}\right], \tag{3.4}$$

where $\boldsymbol{y}$ is the received sequence, and $x(i) \in \{-1, 1\}$ is the $i$-th binary input. The MAP detection decides the value of $x(i)$ according to

$$x(i) = \begin{cases} -1, & \text{if } LAPPR(i) > 0; \\ 1, & \text{otherwise.} \end{cases} \tag{3.5}$$

Though the BCJR algorithm is well proven to be efficient to equalize binary 1-D ISI channel, there is no direct extension to 2-D case.

J. B. Soriaga et al propose iterative multi-strip BCJR approach [43] to calculate the achievable information rates of multilevel codes for binary 2-D ISI channel, which provides an sub-optimal detection algorithm to equalize bianry 2-D ISI channel. In classical multi-strip BCJR algorithm, the whole system is modeled as finite-state system. The previous state on $(i, j)$th output is given by

$$S'(i, j) = \left\{x(i - L_x, j - L_y), x(i - L_x, j - L_y + 1), \cdots, x(i, j - 1)\right\}. \tag{3.6}$$

To be convenient, we denote $\left\{x(i - L_x, j - L_y), x(i - L_x, j - L_y + 1), \cdots, x(i, j - 1)\right\}$ as $\left\{x(i - L_x : i, j - L_y : j - 1)\right\}$. The current state is given by

$$S(i, j) = \left\{x(i - L_x : i, j - L_y + 1 : j)\right\}. \tag{3.7}$$

It can be easily calculated that when $x(i, j)$ is binary, the number of states at $(i, j)$th output is $2^{(L_x \times L_y)}$.

However, when $x(i, j)$ is M-ary, according to (3.6) and (3.7), the number of states at each calculation branch is increased to $M^{(L_x \times L_y)}$. the rapidly increasing number of the states increases the computation complexity significantly and makes the multi-strip BCJR algorithm unaffordable in the sense of computation complexity. To reduce the computation complexity, we propose multistage multi-strip equalization, *i.e.,* using multi-strip BCJR algorithm stage by stage.

To realize MAP detection on every stage, we need to find out the $k$-th level LAPPR of $(i, j)$th output, which is defined by

$$LAPPR^{(k)}(i, j) = \log\left[\frac{P(d^{(k)}(i, j) = -1)|y}{P(d^{(k)}(i, j) = 1|y)}\right]. \tag{3.8}$$

The MAP estimation of $d^{(k)}(i, j)$ is given by

$$d^{(k)}(i, j) = \begin{cases} -1, & \text{if } LAPPR^{(k)}(i, j) > 0; \\ 1, & \text{otherwise.} \end{cases} \tag{3.9}$$

To compute $LAPPR^{(k)}(i, j)$, the number of states is still $M^{(L_x \times L_y)}$. However, similar to classical multi-strip BCJR algorithm, $LAPPR^{(k)}(i, j)$ can be approximated by $L^{(k)}(i, j)$, which is defined as

$$L^{(k)}(i, j) = \sum_{p=0}^{L_x} L(d^{(k)}(i, j)|y(i - p, :)), \tag{3.10}$$

where

$$L(d^{(k)}(i, j)|y(i, :)) = \log\left[\frac{P(d^{(k)}(i, j) = -1)|y(i, :)}{P(d^{(k)}(i, j) = 1|y(i, :))}\right], \tag{3.11}$$

and $y(i, :) = \{y(i, 1),\ y(i, 2), \cdots, y(i, n)\}$.

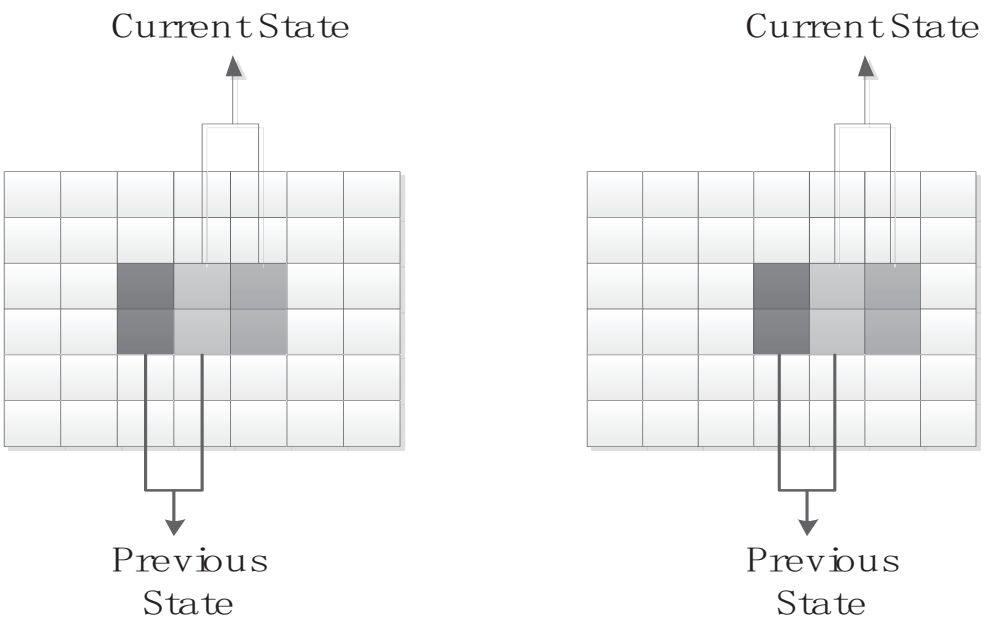
Now the problem has been converted from calculating $LAPPR^{(k)}(i, j)$ to calculating $L^{(k)}(i, j)$. At stage $k$, the input data from level $k + 1$ to level $K$ is already available. If we also know the input data from level 1 to level $k - 1$, then the previous state at stage $k$ should be

$$S'_{(k)}(i, j) = \left\{d^{(k)}(i - L_x : i, j - L_y : j - 1)\right\}, \tag{3.12}$$

and the current state becomes

$$S_{(k)}(i, j) = \left\{d^{(k)}(i - L_x : i, j - L_y + 1 : j)\right\}. \tag{3.13}$$

For example, if the size of the data page is $6 \times 7$ and $L_x = L_y = 2$, then as shown in Figure (3.3(a)), the previous state for the (4, 4)th data is $\{(3, 3), (3, 4), (4, 3), (4, 4)\}$, and the current state for the (4, 4)th data is $\{(3, 4), (3, 5), (4, 4), (4, 5)\}$. For the next data, *i.e.*, the (4, 5)th data, the precious state is changed to $\{(3, 4), (3, 5), (4, 4), (4, 5)\}$ and the current state is $\{(3, 5), (3, 6), (4, 5), (4, 6)\}$ accordingly, which is shown is Figure 3.3(b). Then using multi-strip BCJR algorithm to go through the entire $i$th row, $L(d^{(k)}(i, j)|y(i, :))$ given in (3.11) can be computed.




(a) For (4, 4). (b) For (4, 5)

**Figure 3.3. Previous and current states in multi-strip BCJR**

If our assumption that the data on all levels except level $k$ is available is true, the problem is solved at this point. Also since $d^{(k)}(i, j) \in \{-1, 1\}$ is binary, the number of states is reduced from $(L_x \times L_y)^M$ to $(L_x \times L_y)^2$. But notice that at stage $k$, the input data from level 1 to level $k-1$ is still undecided yet, *i.e.*, those information is still unavailable at stage $k$. How to precalculate the input data from level 1 to level $k-1$ is the problem that needs to be solved to keep the number of states at the value of $(L_x \times L_y)^2$ at stage $k$. This solution of the problem is given as in the following.

### 3.3.2 Gaussian Approximation on Multistage Multi-strip Equalization

The remained problem is how to compute $L^{(k)}(i, j)$ at the channel detector of level k. Notice that from the definition of $L^{(k)}(i, j)$ given in (3.10), $L^{(k)}(i, j)$ can be computed by summing up $L(d^{(k)}(i, j)|y(i-p, :))$ for $p = 0, 1, \cdots, L_x$. The problem is transferred to compute $L(d^{(k)}(i, j)|y(i-p, :))$. According to classical BCJR algorithm the key to calculate

$L(d^{(k)}(i,j)|y(i-p,:))$ is to find out the branch metric of individual BCJR, which is defined by

$$\gamma_{i,j}^{(k)}(s',s) = \log P(y(i,j)|s'_{(k)}(i,j), s_{(k)}(i,j))P(s'_{(k)}(i,j), s_{(k)}(i,j)). \tag{3.14}$$

In (3.14), $P(s'_{(k)}(i,j), s_{(k)}(i,j))$ is easy to be calculated since we assume the input data are *identically independently distributed* (*i.i.d.*). But to compute $P(y(i,j)|s'_{(k)}(i,j), s_{(k)}(i,j))$, we have

$$\begin{aligned}
&P(y(i,j)|s'_{(k)}(i,j), s_{(k)}(i,j)) \\
&= P\left(y(i,j)|\hat{d}^{(k+1:K)}(i-L_y:i, j-L_x, j), d^{(k)}(i-L_y:i, j-L_x, j)\right) \\
&= \frac{1}{2^{k-1}} \sum_{\tilde{d}^{(1:k-1)}(i,j)} P\left(y(i,j)|\hat{d}^{(k+1:K)}(i-L_y:i, j-L_x, j), d^{(k)}(i-L_y:i, j-L_x, j), \tilde{d}^{(1:k-1)}(i,j)\right).
\end{aligned} \tag{3.15}$$

Via (3.15), we need $\tilde{d}^{(1:k-1)}(i,j)$ to calculate $P(y(i,j)|s'_{(k)}(i,j), s_{(k)}(i,j))$, which is still not available at stage k. However according to central limited theorem we can assume that $P\left(y(i,j)|\hat{d}^{(k+1:K)}(i-L_y:i, j-L_x, j), d^{(k)}(i-L_y:i, j-L_x, j)\right)$ approximated follows normal distribution. Hence we give the following proposition

**Proposition 3.3.1** *The distribution of the probability of $y(i,j)$ given the input data on level $k$ and the estimated data from level $k+1$ to $K$ can be approximated as a normal distribution, the approximated distribution is given by*

$$\begin{aligned}
&P\left(y(i,j)|\hat{d}^{(k+1:K)}(i-L_y:i, j-L_x, j), d^{(k)}(i-L_y:i, j-L_x, j)\right) \\
&\quad \sim N\left(\hat{\mu}_{(k)}\left(\tilde{d}^{(1:k-1)}(i,j)\right), \hat{\sigma}^2_{(k)}\left(\tilde{d}^{(1:k-1)}(i,j)\right)\right),
\end{aligned} \tag{3.16}$$

*where*

$$\hat{\mu}_{(k)}\left(\tilde{d}^{(1:k-1)}(i,j)\right) = A_0 + A_1 + \frac{1}{W} \sum_{\tilde{d}^{(1:k-1)}(i-L_x:i, j-L_y:j)} A_2(\tilde{d}^{(1:k-1)}(i-L_x:i, j-L_y:j)), \tag{3.17}$$

*is the mean of the approximated distribution, and*

$$\hat{\sigma}^2_{(k)}\left(\tilde{d}^{(1:k-1)}(i,j)\right) = \frac{1}{W} \sum_{\tilde{d}^{(1:k-1)}(i-L_x:i, j-L_y:j)} \left|A_0 + A_1 + A_2 - \hat{\mu}_{(k)}\left(\tilde{d}^{(1:k-1)}(i,j)\right)\right|^2. \tag{3.18}$$

*is the variance.* $A_0$, $A_1$, *and* $A_2$ *are given by*

$$A_0 = h(0,0)\left[\sum_{k'=k+1}^{K}\sqrt{P^{k'}}\hat{d}^{(k')}(i,j) + \sqrt{P^{k}}d^{(k)}(i,j) + \sum_{k'=1}^{k-1}\sqrt{P^{k'}}\tilde{d}^{(k')}(i,j)\right], \tag{3.19}$$

$$A_1 = \sum_{p=1}^{L_x}\sum_{q=1}^{L_y}h(p,q)\left[\sum_{k'=k+1}^{K}\sqrt{P^{k'}}\hat{d}^{(k')}(i,j) + \sqrt{P^{k}}d^{(k)}(i,j)\right], \tag{3.20}$$

$$A_2\left(\tilde{d}^{(1:k-1)}(i-L_x:i, j-L_y:j)\right) = \sum_{p=1}^{L_x}\sum_{q=1}^{L_y}h(p,q)\left[\sum_{k'=1}^{k-1}\sqrt{P^{k'}}\tilde{d}^{(k')}(i-p, j-q)\right]. \tag{3.21}$$

$W$ *is the number of possible combinations of* $\left\{\tilde{d}^{(1:k-1)}(i-L_x:i, j-L_y:j)\right\}$.

Combining (3.15) and (3.16), we have

$$P(y(i,j)|s'_{(k)}(i,j), s_{(k)}(i,j)) \approx \frac{1}{2^{K-k}}\frac{1}{2\pi\hat{\sigma}^2_{(k)}}\sum_{\tilde{d}^{(1:k-1)}(i,j)}\exp\left\{-\frac{\left(y(i,j)-\hat{\mu}_{(k)}\left(\tilde{d}^{(1:k-1)}(i,j)\right)\right)^2}{2\hat{\sigma}^2_{(k)}\left(\tilde{d}^{(1:k-1)}(i,j)\right)}\right\}. \tag{3.22}$$

Notice that both $\hat{\mu}_{(k)}\left(\tilde{d}^{(1:k-1)}(i,j)\right)$ and $\hat{\sigma}^2_{(k)}\left(\tilde{d}^{(1:k-1)}(i,j)\right)$ can be computed off line. Therefore, the number of states in stage $k$ keeps at $(L_x \times L_y)^2$.

### 3.3.3 Detection Steps

The details of the complete equalization algorithm are summarized as follows:

1. The 2-D ISI channel can be modeled as a Markov channel with finite-state machine. The previous state of the $(i, j)$ pixel at level $k$ $S'_{(k)}(i,j)$ is defined in (3.12), and the current state $S_{(k)}(i,j)$ is given by (3.13);

2. Since we adopt multistage equalization, at any given level $k$, the data from level $k+1$ to level $K$ should be available at decoding stage $k$;

3. The branch metric of individual BCJR $\gamma^{(k)}_{i,j}(s', s)$ can be approximated via (3.22);

4. Carry the multi-strip BCJR algorithm on level $k$ based on the branch metric $\gamma^{(k)}_{i,j}(s', s)$ to compute $L(d^{(k)}(i,j)|y(i,:))$;

5. $L^{(k)}(i,j)$ is computed via (3.10);

6. Pass $L^{(k)}(i, j)$ to the decoder at level $k$.

Notice that in the proposed Gaussian approximated multi-stage multi-strip equalization algorithm, we avoid computing the exact value of $P(y(i, j)|s'_{(k)}(i, j), s_{(k)}(i, j))$. Instead we equalize the channel stage by stage by computing $L^{(k)}(i, j)$ defined in (3.10). On each stage, based on central limited theorem, the distribution of
$P\left(y(i, j)|\hat{d}^{(k+1:K)}(i - L_y : i, j - L_x, j), d^{(k)}(i - L_y : i, j - L_x, j)\right)$ is approximated by a normal distribution, the mean and variance of which can be computed offline via (3.17) and (3.18), respectively. Hence the number of states at each stage is reduced from $M^{L_x \times L_y}$ to $2^{L_x \times L_y}$ [45].

## 3.4 Achievable Information Rate

In section 3.3, we propose an equalization algorithm to equalize M-ary 2-D ISI channel. However to further reduce the detection error probability, the channel code needs to be designed, through which the detection error goes to zero with infinite length of codewords. From information theory, we know that with the same codeword length, the more redundancy you add to the original transmitted information, the smaller the bit error rate is. But extra redundancy reduces the transmission efficiency. How to find out the minimum information redundancy such that the detection error still goes to zero with infinite codeword length is the problem discussed in this section.

First, we give the definition of *achievable information rate* (AIR) with the equalization approach proposed in section 3.3.

**Definition 3.4.1** *The AIR at level k is the* mutual information *(MI) between the inputs on the k-th level and the soft information given by the proposed equalization approach, which is* $L^{(k)}(i, j)$ *in our system.*

By the definition, we have

$$\begin{aligned}
&\mathcal{I}\left(d^{(k)}(i,j);L^{(k)}(i,j)\right)\\
&=\mathcal{H}\left(L^{(k)}(i,j)\right)-\mathcal{H}\left(L^{(k)}(i,j)|d^{(k)}(i,j)\right)\\
&=-E\left[\log_2 P\left(L^{(k)}(i,j)\right)\right]+E\left[\log_2 P\left(L^{(k)}(i,j)|d^{(k)}(i,j)\right)\right]\\
&=-\int P\left(L^{(k)}(i,j)\right)\log_2 P\left(L^{(k)}(i,j)\right)dL^{(k)}(i,j)\\
&\quad+\int P\left(L^{(k)}(i,j)|d^{(k)}(i,j)\right)\log_2 P\left(L^{(k)}(i,j)|d^{(k)}(i,j)\right)dL^{(k)}(i,j)|d^{(k)}(i,j)
\end{aligned}\tag{3.23}$$

where $\mathcal{I}\left(d^{(k)}(i,j);L^{(k)}(i,j)\right)$ represents the mutual information between $d^{(k)}(i,j)$ and $L^{(k)}(i,j)$, and $\mathcal{H}\left(L^{(k)}(i,j)\right)$ is the entropy of $L^{(k)}(i,j)$. $P\left(L^{(k)}(i,j)\right)$ is the *probability density function* (pdf) of $L^{(k)}(i,j)$. $E\left[\log_2 P\left(L^{(k)}(i,j)\right)\right]$ is the expectation value of $\log_2 P\left(L^{(k)}(i,j)\right)$.

(3.23) provides a method to calculate the AIR by Monte-Carlo simulation, which is summarized as the following:

1. Simulate the transmission over the M-ary 2-D ISI channel $N$ times with *i.i.d.* M-ary input symbols.

2. For each simulation, on every equalization stage, calculate $L^{(k)}(i,j)$ by following the proposed multi-stage multi-strip Gaussian approximated equalization algorithm.

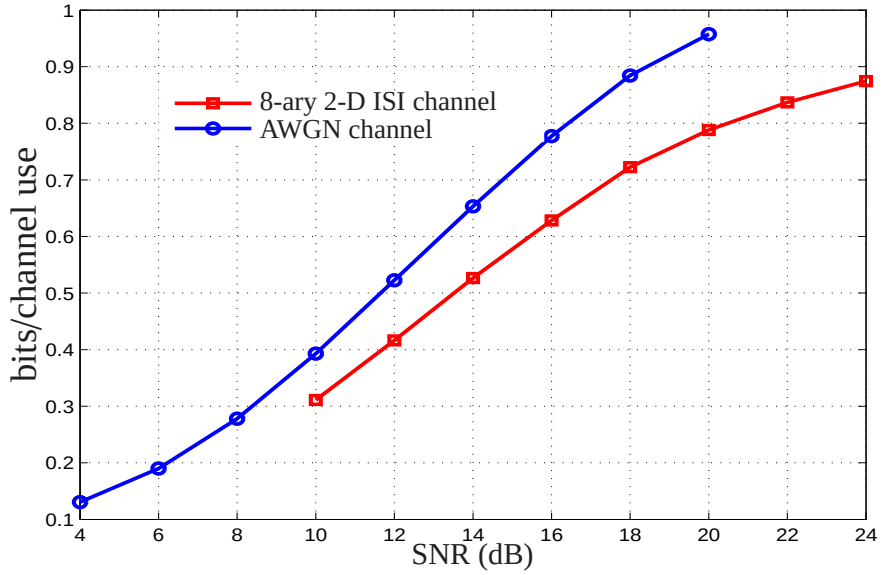
3. Generate the histograms of $L^{(k)}(i,j)$ and $L^{(k)}(i,j)|d^{(k)}(i,j)$ with the simulation results.

4. Estimate $P\left(L^{(k)}(i,j)\right)$ and $P\left(L^{(k)}(i,j)|d^{(k)}(i,j)\right)$ accordingly by using kernel function on the corresponding histogram.

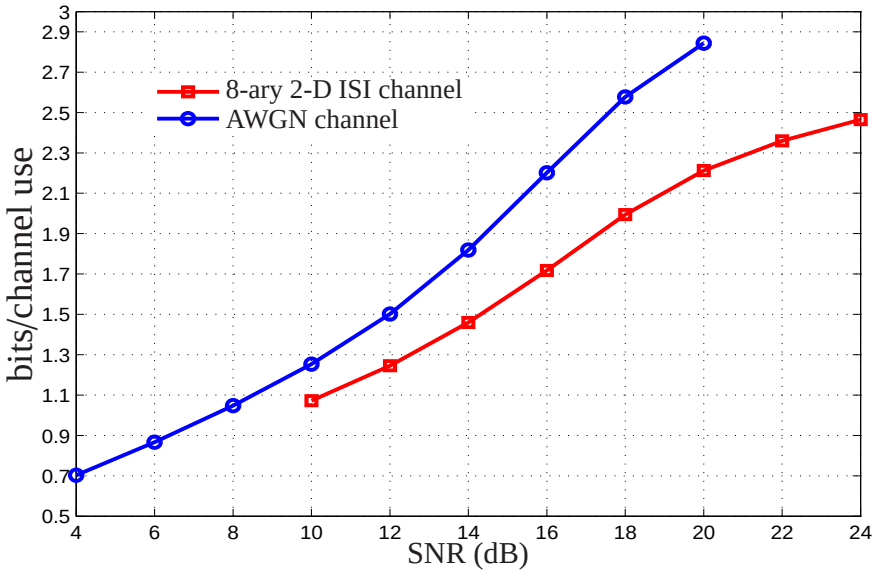
5. Plugging the estimated $P\left(L^{(k)}(i,j)\right)$ and $P\left(L^{(k)}(i,j)|d^{(k)}(i,j)\right)$ in (3.23) to compute the AIR of level $k$.

Notice that there should be no encoding in the scheme when we compute the AIR, which means $d^{(k)}(i,j)$ is *i.i.d.* data without any coding gains.

Figure 3.4 shows the numerical results of AIR with different SNRs, where the channel response $h = \frac{1}{\sqrt{18.25}} \begin{bmatrix} 4 & 1 \\ 1 & 0.5 \end{bmatrix}$ and $M = 8$. Figure 3.4(a) and Figure 3.4(b), respectively, shows the AIR at level 2 and the total AIR of the total $\log_2 M = 3$ levels. The AIR with the ISI-free *additive white Gaussian noise* (AWGN) channel is also plotted for comparison. On level 2, when SNR is 12 dB, the gap between the Gaussian channel and 8-ary 2-D ISI channel is about 0.1bits per channel use. The gap is caused by two factors. The first one is that 2-D ISI channel has 2-D interference between symbols. Hence with the same SNR, Gaussian channel definitely has much higher channel capacity than 2-D ISI channel. Furthermore, since there is no interference in Gaussian channel, the 2-D Gaussian channel can be modeled as parallel scaler Gaussian channels. In other words, 2-D Gaussian is equivalent to parallel 1-D Gaussian channel, which reduce the channel dimension of transmission from two to one. The second reason causes the gap is that the proposed Gaussian-approximated equalization algorithm is a sub-optimal equalization approach, which means the decisions given by the Gaussian-approximated equalization are not MAP decisions. However, the presented detection approach offers a sub-optimal way to efficiently equalize M-ary 2-D ISI channel.




(a) AIR of level 2.

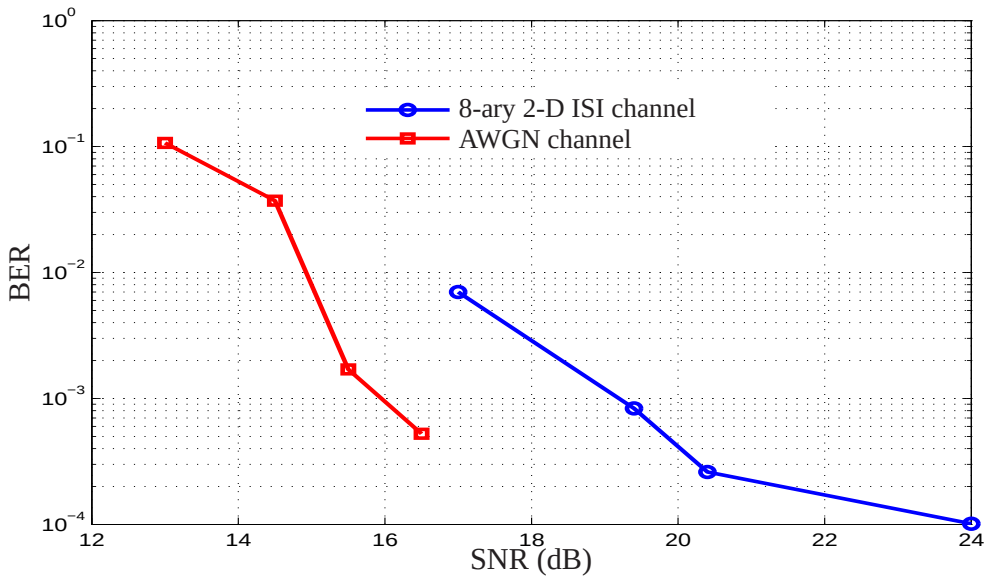



(b) Total AIR of 3 levels.

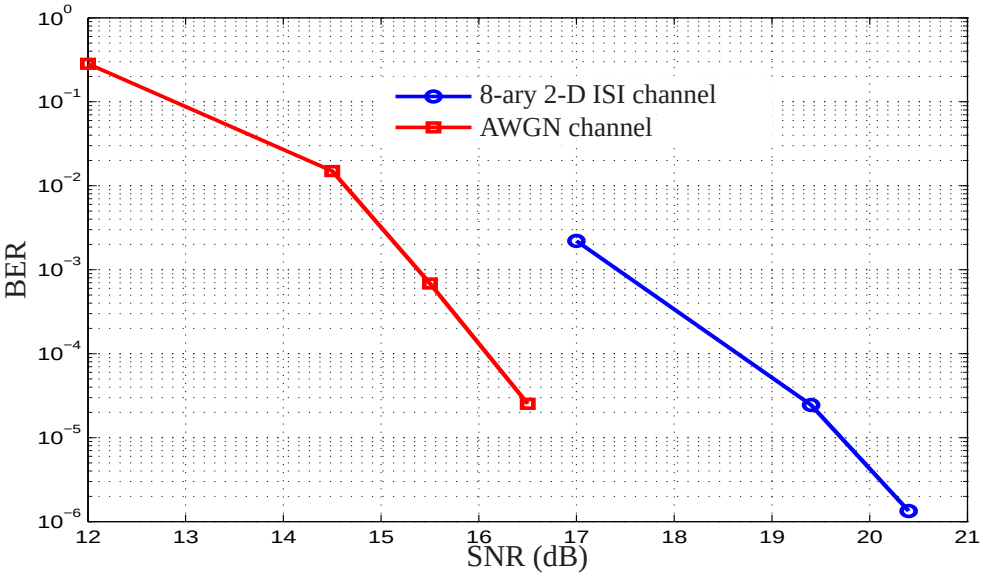
**Figure 3.4. Comparison of AIRs between AWGN channel and M-ary 2-D ISI channel.**

## 3.5 Code Design and Simulation Results

Semi-algebraic LDPC [69] component codes with code rates 0.4, 0.7 and 0.8 for level 1, level 2, and level 3, respectively, are used in the scheme. With the condition of perfectly decoded bits of the previous stage, the averaged BER performance of the multilevel codes is shown in Figure 3.5(a). The performance of the proposed scheme in the 2-D ISI channel is about 2.3 dB inferior to the AWGN channel. Figure 3.5(b) shows the performance at level 2, which is less than 1.8 dB inferior to the AWGN channel with the perfect feedback from level 3.




(a) The average BER of 3 levels.




(b) BER of level 2.

**Figure 3.5. BER performance with semi-algebraic LDPC codes.**

## 3.6 Conclusion

In this chapter, we have investigated a new multilevel coding and multistage decoding scheme for M-ary 2-D ISI channel. The fundamental idea is to decode the input stage by stage. In each stage, based on the soft and hard decoding results of the decoded levels, the BCJR algorithm is employed iteratively through the strips of the data page as in [43]. To reduce the computation complexity to an affordable level, in each stage, instead of applying the full-branch BCJR algorithm, the BCJR algorithm is only employed on reduced states by considering the bits from the undecoded levels as independently and identically distributed with equal probability. In this presented approach, the computation complexity for each stage is reduced $M^{L_x \times L_y}$ to $2^{L_x \times L_y}$ [45]. Such huge complexity reduction makes the computation affordable and practical.

# CHAPTER 4

# INFORMATION RATE LOSS INDUCED BY MAXIMUM-LIKELIHOOD AND ZERO-FORCING DETECTORS

Multiple-Input, Multiple-Output (MIMO) systems have received a great deal of attention because of the increase in the transmitted information rate and reliability. Existing results on fundamental limits of MIMO systems are focused on the assumption of continuous signals at the receiver side and the effect of detectors has largely not been addressed. However, in practical digital communication systems, when the inputs are discrete the continuous outputs given by the receivers have to be mapped to the alphabet of the transmitted signals, *i.e.* the final outputs should also have discrete values. We refer to the ML (ZF) receiver with the hard mapping step as the ML (ZF) detector and call the hard outputs given by detectors as the detected signals. The hard detection step has not been considered before in the related work.

In this chapter, we focus our study on the *mutual information* (MI) of the discrete MIMO channels with two widely adopted detectors, one is the MLD and the other is the ZFD. To differentiate from the MI without hard mapping step, we refer the one here as *post-detection mutual information* (PMI). We need to emphasize that the PMI which we consider in this paper is the MI between two specific discrete vectors which belong to finite alphabets, *i.e.*, one vector is the transmitted discrete vector, the other is the hard detected vector given by MLD or ZFD. We first establish the definition and analytical expression of the PMI with MLD and ZFD. We observe that there is no closed form for the PMI with MLD or ZFD. However, when *phase-shift keying* (PSK) symbols are employed, we present an asymptotically tight lower bound of the PMI with MLD or ZFD . The lower bounds are easily computed which allows us to evaluate the ultimate achievable information rates for MIMO systems with detectors. Furthermore, when *quadrature amplitude modulation* (QAM) symbols are employed, we provide a simple numerical method to compute the

PMI with ZFD which is shown to exactly match the simulation results. Since the hard mapping step in the detector is irreversible, we expect that the PMI is reduced compared to the MI without hard mapping. The conclusion is confirmed by both the simulation and the theoretic results. Consequently, the ultimate achievable PMI rates that can be transmitted through the MIMO channels with MLD or ZFD serve as more practical benchmarks for transmissions.

The rest of the chapter is organized as follows. In Section 4.1, we review the general MIMO channel model as well as the definitions for MLD and ZFD discussed in the chapter. Moreover, we give the definition of PMI and explore the meaning of PMI. In Section 4.2 we derive the lower bound of the PMI with MLD when the inputs are chosen from PSK symbols. Section 4.3 first presents the lower bound of the PMI with ZFD when PSK symbols are used, and then the numerical expression of the PMI with ZFD employing QAM symbols is derived. Simulation results are presented in Section 4.5 and Section 4.6 concludes the chapter.

## 4.1 Problem Formulation

In this section, we first give the system model, and then present the problem itself and the meaning of the problem. *Post-detection mutual information* (PMI) is introduced, which will be shown later, as the more practical bench mark in MIMO system with detectors.

### 4.1.1 System Model and Problem Formulation

In this section, we review the system model, which is discussed in this chapter. For a discrete-time MIMO channel with $M$ transmitters and $N$ receivers, the relationship between the output $\boldsymbol{y}$, the input symbol $\boldsymbol{s}$, and the channel response $\boldsymbol{H}$ is given by

$$\boldsymbol{y} = \boldsymbol{H}\boldsymbol{s} + \boldsymbol{\omega}, \tag{4.1}$$

where $\boldsymbol{y}$ is the $N \times 1$ vector, $\boldsymbol{s}$ is the $M \times 1$ transmitted signal, $\boldsymbol{H}$ is an $N \times M$ complex Gaussian distributed channel matrix, and $\boldsymbol{\omega}$ is *i.i.d.* zero-mean complex Gaussian noise

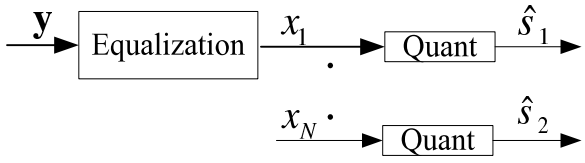
with covariance matrix $E[\boldsymbol{\omega}\boldsymbol{\omega}^{\mathcal{H}}] = \sigma_{\omega}^2 \boldsymbol{I}_N$. In the following discussion we focus on the case of $M = N$.

Let $s_k$ be the $k$-th element of $\boldsymbol{s}$, which is drawn from complex QAM or PSK constellation $\mathcal{S}$ with equal probability. The SNR of the channel is defined as

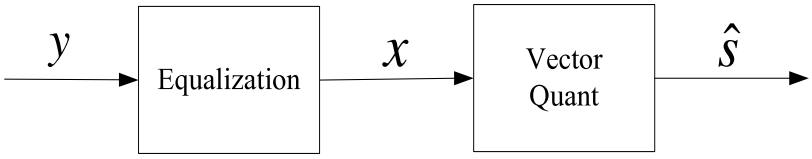
$$SNR = \frac{E_s}{N_0}, \tag{4.2}$$

where $E_s = E[|s_k|^2]$ and $N_0 = 2\sigma_{\omega}^2$.

We define that the detection process includes equalizing the received vector $\boldsymbol{y}$ and hard mapping the equalized vector to finite constellation.




(a) The scheme of ZFD.




(b) The scheme of MLD.

**Figure 4.1. The scheme of ZFD and MLD.**

The structure of ZFD is shown in Figure 4.1(a). The first step is equalizing the received vector $\boldsymbol{y}$, which is given as

$$\boldsymbol{x} = \boldsymbol{H}^{\dagger}\boldsymbol{y} = \boldsymbol{s} + \boldsymbol{\eta}, \tag{4.3}$$

where $\boldsymbol{H}^{\dagger} = (\boldsymbol{H}^{\mathcal{H}}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathcal{H}}$, $\boldsymbol{x}$ is the equalized vector, and $\boldsymbol{\eta} = \boldsymbol{H}^{\dagger}\boldsymbol{\omega}$. The covariance matrix of the equalized noise $\boldsymbol{\eta}$ is

$$\boldsymbol{W} = E[\boldsymbol{\eta}\boldsymbol{\eta}^{\mathcal{H}}] = \boldsymbol{H}^{\dagger}(\boldsymbol{H}^{\dagger})^{\mathcal{H}} E[\boldsymbol{\omega}\boldsymbol{\omega}^{\mathcal{H}}] = \sigma_{\omega}^2 (\boldsymbol{H}^{\mathcal{H}}\boldsymbol{H})^{-1}. \tag{4.4}$$

As shown in (4.4), the equalization introduces the correlation among the noise entries. However, in the hard mapping step of the ZFD, the correlations among the noise entries

are not considered. The ZFD maps $\boldsymbol{x}$ symbol by symbol. For example, the $k$-th entry of $\boldsymbol{x}$ denoted as $x_k$ is mapped to the alphabet $\mathcal{S}$ by

$$\hat{s}_k = \mathfrak{Q}_s(x_k) = \underset{\tilde{s}_k \in \mathcal{S}}{\arg\min} \|x_k - \tilde{s}_k\|^2, \ k = 1, \cdots, N, \tag{4.5}$$

where $\mathfrak{Q}_s(\cdot)$ represents the hard mapping operation of ZFD, and $\hat{s}_k$ is the $k$-th detected symbol of the detected signal $\hat{\boldsymbol{s}}_{ZF}$ given by ZFD.

Different from ZFD, MLD directly maps the received vector $\boldsymbol{y}$ to an M-dimensional space $\mathcal{S}^M$, i.e.,

$$\hat{\boldsymbol{s}}_{ML} = \mathfrak{Q}_v(\boldsymbol{y}) = \underset{\tilde{\boldsymbol{s}} \in \mathcal{S}^M}{\arg\min} \|\boldsymbol{y} - \boldsymbol{H}\tilde{\boldsymbol{s}}\|^2, \tag{4.6}$$

where $\mathfrak{Q}_v(\cdot)$ represents the hard mapping operation of MLD and $\hat{\boldsymbol{s}}_{ML}$ is the final detected signal given by MLD. The hard mapping operation of MLD given in (4.6) is equivalent to quantizing the equalized vector $\boldsymbol{x}$ to $\mathcal{S}^M$. The equivalent form of (4.6) is

$$\hat{\boldsymbol{s}}_{ML} = \mathfrak{Q}_v(\boldsymbol{x}) = \underset{\tilde{\boldsymbol{s}} \in \mathcal{S}^M}{\arg\min} \left(\boldsymbol{x} - \tilde{\boldsymbol{s}}\right)^{\mathcal{H}} \boldsymbol{W}^{-1} \left(\boldsymbol{x} - \tilde{\boldsymbol{s}}\right), \tag{4.7}$$

and the structure of the equivalent MLD is shown in Figure 4.1(b).

The question is what is the mutual information between the input symbols $\boldsymbol{s}$ and the estimated symbols $\hat{\boldsymbol{s}}_{ML}/\hat{\boldsymbol{s}}_{ZF}$ given by MLD/ZFD. As reviewed in Chapter 2,all the existing results have not considered the information loss in the final hard mapping step in the detection. However the information loss in the hard mapping step does exit and affect the detection. This chapter answer the question by quantifying the information loss induced by the hard mapping step. The information loss that has been neglected before actually confirms that the achievable information rate with MLD or ZFD should be less than the known value.

### 4.1.2 The definition and meaning of PMI

To consider the ignored information rate loss, we introduce a new metric, which is *post-detection mutual information* (PMI), to quantify the ultimate information rate that can be achieved in MIMO system with detectors. First, we give the definition of PMI.

**Definition 4.1.1** *When $\boldsymbol{H}$ is known, the PMI of a MIMO system with MLD or ZFD is, respectively, the mutual information between the transmitted signal and the hard detected signal given by MLD or ZFD, i.e., the PMI with MLD is $\mathcal{I}(\boldsymbol{s}; \hat{\boldsymbol{s}}_{ML}|\boldsymbol{H})$, while the PMI with ZFD is $\mathcal{I}(\boldsymbol{s}; \hat{\boldsymbol{s}}_{ZF}|\boldsymbol{H})$.*

Now let us explore the meaning of PMI. Consider a widely used MIMO system with receivers and error-control coding. The ML or ZF receiver computes the log-likelihood ratio (LLR) of each bit of the transmitted symbols based on the raw resulting outputs of the channel and the channel response. The LLRs are transferred to the decoder as the priori information for decoding. Next, the decoders compute the LLR of each bit based on the priori information provided by the receiver. Finally, the hard decoded bits are determined via the LLR given by the decoders. When we design the error-control codes, we need to ask what code rates should be used. Obviously, the highest achievable code rates should be the ultimate achievable information rates of the systems. From Shannon's theorem we know that the ultimate achievable information rates of a communication system should be the MI between the inputs and outputs of that system without coding gains. For MIMO systems with an ML or ZF receiver, since the final hard decoding step of the decoder should be taken into account, the ultimate achievable code rates of the system are no longer the MI between the discrete inputs and the continuous outputs given by the receivers [29]. Instead, the ultimate achievable code rates of the MIMO systems with an ML or ZF receiver should be equivalent to the MI between the discrete inputs and the discrete outputs of the MIMO systems with MLD or ZFD, respectively. Therefore, the PMI is actually the highest code rates that we can apply in MIMO systems with an ML or ZF receiver [**?**, 70]. The goal of our work is to find the value of it.

## 4.2 Post-Detection Mutual Information with Maximum-Likelihood Detector

In this section, we first consider the MIMO systems with MLD and develop the analytical expression of the PMI with MLD defined in (4.6) or (4.7). We assume perfect channel knowledge is available at the receiver and the input symbols are uniformly distributed over the finite alphabet $\mathcal{S}$. We develop the PMI with MLD based on the definition of it. Note that the channel has discrete input discrete output under the definition of the MLD.

**Proposition 4.2.1** *When PSK symbols are transmitted, the PMI of a MIMO system with MLD is given by*

$$\mathcal{I}(\boldsymbol{s};\hat{\mathbf{s}}_{ML}|\boldsymbol{H}) = M\log_2 q + \frac{1}{q^M}\sum_{\boldsymbol{s}_u\in\mathcal{S}^M}\sum_{\boldsymbol{s}_v\in\mathcal{S}^M}\left(P(\hat{\mathbf{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})\cdot\log_2 P(\hat{\mathbf{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})\right), \tag{4.8}$$

*where $q$ is the size of the PSK constellation $\mathcal{S}$, $\boldsymbol{s}$ is the transmitted signal vector and $\hat{\mathbf{s}}_{ML}$ given in (4.6) or (4.7) is the detected vector with MLD.*

Actually, because of the correlation between the transmitted symbols, there is no closed form to get the PMI with MLD. But when PSK symbols are employed, the symbols have equal energy and they can be exchanged with each other without changing the performance of the system. Therefore, in this section we focus on PSK symbols to derive a lower bound of the PMI with MLD.

From (4.8), we observe that both $\boldsymbol{s}$ and $\hat{\mathbf{s}}_{ML}$ are discrete (belonging to finite alphabets), and thus the PMI is no longer calculated by the integral of some probability density function (PDF). Instead, it is expressed by the error and correct detection probabilities. The error probability is defined as the probability that the detected signal vector $\hat{\mathbf{s}}_{ML}$ is $\boldsymbol{s}_v$ but the transmitted signal vector $\boldsymbol{s}$ is $\boldsymbol{s}_u$. The correct detection probability is the probability that the detection signal vector is exactly the transmitted signal vector. It is obvious from (4.8) that the key point to calculate the PMI is to know both the error and correct detection probabilities.

Let us work on the error probability first. According to the definition of the MLD given in (4.7) we have

$$\begin{aligned} & P(\hat{\boldsymbol{s}}_{ML} = \boldsymbol{s}_v | \boldsymbol{s} = \boldsymbol{s}_u, u \neq v, \boldsymbol{H}) \\ &= P\left( \|\boldsymbol{x} - \boldsymbol{s}_v\|^2_{\boldsymbol{W}^{-1}} \leq \|\boldsymbol{x} - \boldsymbol{s}_k\|^2_{\boldsymbol{W}^{-1}}, \forall k \neq v \middle| \boldsymbol{s} = \boldsymbol{s}_u \right) \\ &= P\left( \max\left( \|\boldsymbol{x} - \boldsymbol{s}_v\|^2_{\boldsymbol{W}^{-1}} - \|\boldsymbol{x} - \boldsymbol{s}_k\|^2_{\boldsymbol{W}^{-1}} \right) \leq 0, \forall k \neq v \middle| \boldsymbol{s} = \boldsymbol{s}_u \right), \end{aligned} \tag{4.9}$$

where

$$\|\boldsymbol{x} - \boldsymbol{s}_k\|^2_{\boldsymbol{W}^{-1}} = (\boldsymbol{x} - \boldsymbol{s}_k)^{\mathcal{H}} \boldsymbol{W}^{-1} (\boldsymbol{x} - \boldsymbol{s}_k). \tag{4.10}$$

If the covariance matrix $\boldsymbol{W}$ is a diagonal matrix, then the two events $\|\boldsymbol{x} - \boldsymbol{s}_v\|^2_{\boldsymbol{W}^{-1}} \leq \|\boldsymbol{x} - \boldsymbol{s}_{k1}\|^2_{\boldsymbol{W}^{-1}}$ and $\|\boldsymbol{x} - \boldsymbol{s}_v\|^2_{\boldsymbol{W}^{-1}} \leq \|\boldsymbol{x} - \boldsymbol{s}_{k2}\|^2_{\boldsymbol{W}^{-1}}$, $k1 \neq k2 \neq v$, are independent to each other, and thus the error probability can be computed by

$$\begin{aligned} & P(\hat{\boldsymbol{s}}_{ML} = \boldsymbol{s}_v | \boldsymbol{s} = \boldsymbol{s}_u, u \neq v, \boldsymbol{H}) \\ &= P\left( \max\left( \|\boldsymbol{x} - \boldsymbol{s}_v\|^2_{\boldsymbol{W}^{-1}} - \|\boldsymbol{x} - \boldsymbol{s}_k\|^2_{\boldsymbol{W}^{-1}} \right) \leq 0, \forall k \neq v \middle| \boldsymbol{s} = \boldsymbol{s}_u \right) \\ &= \prod_{\forall k \neq v, \boldsymbol{s} = \boldsymbol{s}_u} P\left( \|\boldsymbol{x} - \boldsymbol{s}_v\|^2_{\boldsymbol{W}^{-1}} \leq \|\boldsymbol{x} - \boldsymbol{s}_k\|^2_{\boldsymbol{W}^{-1}} \middle| \boldsymbol{s} = \boldsymbol{s}_u \right), \end{aligned} \tag{4.11}$$

where $P\left( \|\boldsymbol{x} - \boldsymbol{s}_v\|^2_{\boldsymbol{W}^{-1}} \leq \|\boldsymbol{x} - \boldsymbol{s}_k\|^2_{\boldsymbol{W}^{-1}} \middle| \boldsymbol{s} = \boldsymbol{s}_u \right)$ is the pair-wise error probability given $\boldsymbol{s} = \boldsymbol{s}_u$. Lemma 4.2.2 in the following provides the method to compute the pair-wise error probability.

**Lemma 4.2.2** *Given the system model in (2.3), when $\boldsymbol{s} = \boldsymbol{s}_u$ we have*

$$P\left( \|\boldsymbol{x} - \boldsymbol{s}_v\|^2_{\boldsymbol{W}^{-1}} \leq \|\boldsymbol{x} - \boldsymbol{s}_u\|^2_{\boldsymbol{W}^{-1}} \right) = Q\Big( \frac{\mu_{ML}(uv)}{\sigma_{ML}(uv)} \Big) = Q\Big( \frac{\sigma_{ML}(uv)}{2} \Big) \tag{4.12}$$

*where $Q(x) = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}} \exp(-\frac{t^2}{2}) dt$ is the Q function, $\mu_{ML}(uv)$ and $\sigma^2_{ML}(uv)$ are determined as*

$$\mu_{ML}(uv) = \|\boldsymbol{s}_u - \boldsymbol{s}_v\|^2_{\boldsymbol{W}^{-1}}, \text{ and } \sigma^2_{ML}(uv) = 2\|\boldsymbol{s}_u - \boldsymbol{s}_v\|^2_{\boldsymbol{W}^{-1}}. \tag{4.13}$$

Unfortunately, the covariance matrix $\boldsymbol{W}$ is usually a non-diagonal one, which makes the two events $\|\boldsymbol{x} - \boldsymbol{s}_v\|^2_{\boldsymbol{W}^{-1}} \leq \|\boldsymbol{x} - \boldsymbol{s}_{k1}\|^2_{\boldsymbol{W}^{-1}}$ and $\|\boldsymbol{x} - \boldsymbol{s}_v\|^2_{\boldsymbol{W}^{-1}} \leq \|\boldsymbol{x} - \boldsymbol{s}_{k2}\|^2_{\boldsymbol{W}^{-1}}$, $k1 \neq k2 \neq v$, not

independent to each other any more. Under such conditions, (4.11) can not hold. How to get the error probability with a non-diagonal covariance matrix is the problem we need to solve now. When $\boldsymbol{W}$ is non-diagonal, there is no closed form for the error probability given in (4.9). However, a simple asymptotically tight bound for the error probability is presented in the following lemma.

**Lemma 4.2.3** *Given the system model in (2.3), the MLD in (4.7) and the transmitted signal* $\boldsymbol{s} = \boldsymbol{s}_u$*, we have*

$$\begin{aligned} P(\hat{\boldsymbol{s}}_{ML} = \boldsymbol{s}_v | \boldsymbol{s} = \boldsymbol{s}_u, u \neq v, \boldsymbol{H}) &\leq Q\Big(\frac{\mu_{ML}(uv)}{\sigma_{ML}(uv)}\Big) \\ &= Q\Big(\frac{\sigma_{ML}(uv)}{2}\Big), \end{aligned} \tag{4.14}$$

*where* $\mu_{ML}(uv)$ *and* $\sigma^2_{ML}(uv)$ *are given in (4.13).*

Now we give some numerical examples to verify how well the upper bound given in lemma 4.2.3 approaches the true error probability.

*Example 1:* We examine how well the PDF of the normal distribution with mean $\mu_{ML}(uv)$ and variance $\sigma^2_{ML}(uv)$ matches the real PDF of $D_{max}$, where

$$D_{max}(u, v) = \max\left(\|\boldsymbol{x} - \boldsymbol{s}_v\|^2_{\boldsymbol{W}^{-1}} - \|\boldsymbol{x} - \boldsymbol{s}_k\|^2_{\boldsymbol{W}^{-1}}, \forall k \neq v | \boldsymbol{s} = \boldsymbol{s}_u\right). \tag{4.15}$$

Actually, the normal PDF with mean $\mu_{ML}(uv)$ and variance $\sigma^2_{ML}(uv)$ is the PDF of the distribution of the upper bound of the pair-wise error probability given in *Lemma 2*. The real PDF of $D_{max}$ is obtained by plotting the histogram which is achieved by recording $D_{max}$ for $50,000$ random realizations of the channel. In this example, 4-PSK symbols are employed.

First, we examine $2 \times 2$ MIMO channels. Two channel matrices $\boldsymbol{H}_{a1}$ and $\boldsymbol{H}_{a2}$ are randomly generated which are given by

$$\boldsymbol{H}_{a1} = \begin{bmatrix} 1.0878 + 0.9618i & -1.1143 + 2.5323i \\ -0.1578 - 0.4552i & -0.2035 + 1.2493i \end{bmatrix} \tag{4.16}$$

and

$$\boldsymbol{H}_{a2} = \begin{bmatrix} -0.3089 - 0.9641i & -0.7504 + 0.7232i \\ -1.2150 + 0.7858i & -1.3505 - 1.2916i \end{bmatrix}. \tag{4.17}$$

The results are plotted in Fig. 4.2. We observe that at $SNR = 2dB$ for both $\boldsymbol{H}_{a1}$ and $\boldsymbol{H}_{a2}$ the PDFs of the upper bound match well with the histograms from simulation. But when $SNR$ decreases to $-8dB$, there exists a gap between the two PDFs.

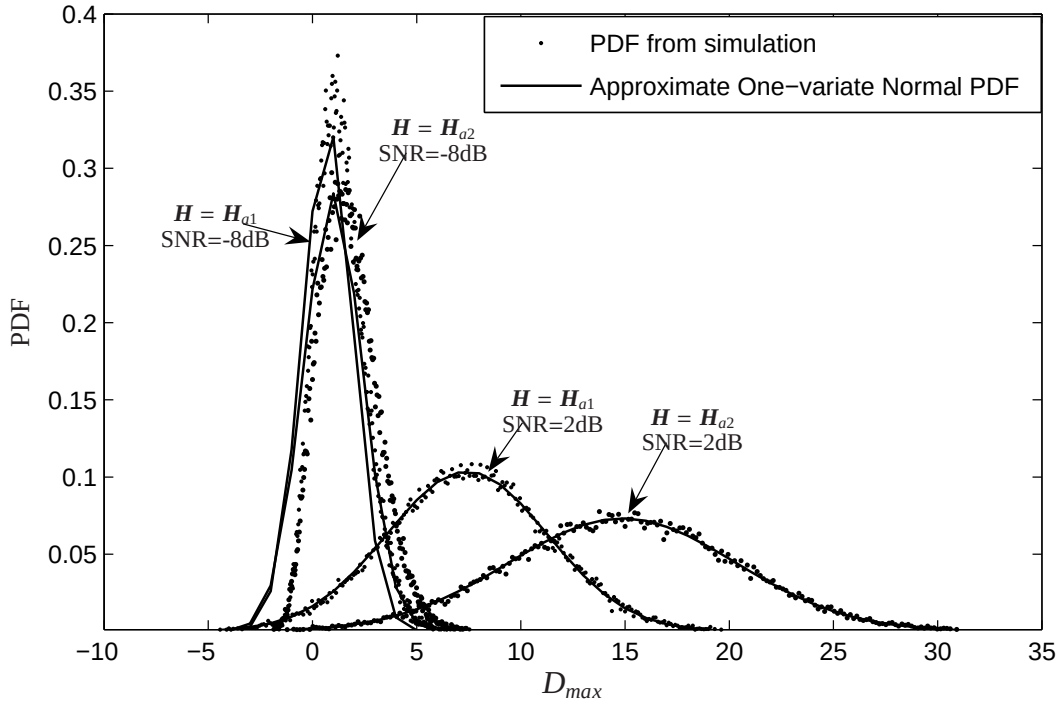



**Figure 4.2. PDFs of $D_{max}$ with $M = N = 2$.**

Next, $3 \times 3$ MIMO channels are examined with the following two randomly generated channel matrices

$$\boldsymbol{H}_{b1} = \begin{bmatrix} 0.6792 + 0.2844i & 0.7559 + 0.4947i & 1.3339 + 0.0198i \\ -1.7443 - 0.0395i & 2.0962 - 0.0071i & -0.3162 - 0.0469i \\ 0.4740 + 0.4906i & -0.3300 - 0.4790i & 0.8787 - 0.5347i \end{bmatrix} \tag{4.18}$$

and

$$\boldsymbol{H}_{b2} = \begin{bmatrix} 0.8719 + 1.4839i & 1.0838 - 2.1562i & 0.4023 + 1.1080i \\ 2.0051 - 1.0058i & 1.4087 + 0.2904i & 0.4147 - 0.3758i \\ 0.0731 - 1.8752i & -0.4578 + 1.2118i & -1.0468 + 1.3289i \end{bmatrix}. \tag{4.19}$$

The results are shown in Fig. 4.3. Similar to the results in Fig. 4.2, the PDFs of the upper bound still match well with the PDFs from the simulations when $SNR = 2dB$. But the gap emerges when $SNR = -8dB$. On the other hand, it is also observed from both Fig. 4.2 and Fig. 4.3 that the numbers of transmitters and receivers do not affect how tight the upper bound is. Therefore the example verifies the effectiveness of the conclusion of *Lemma 2*.

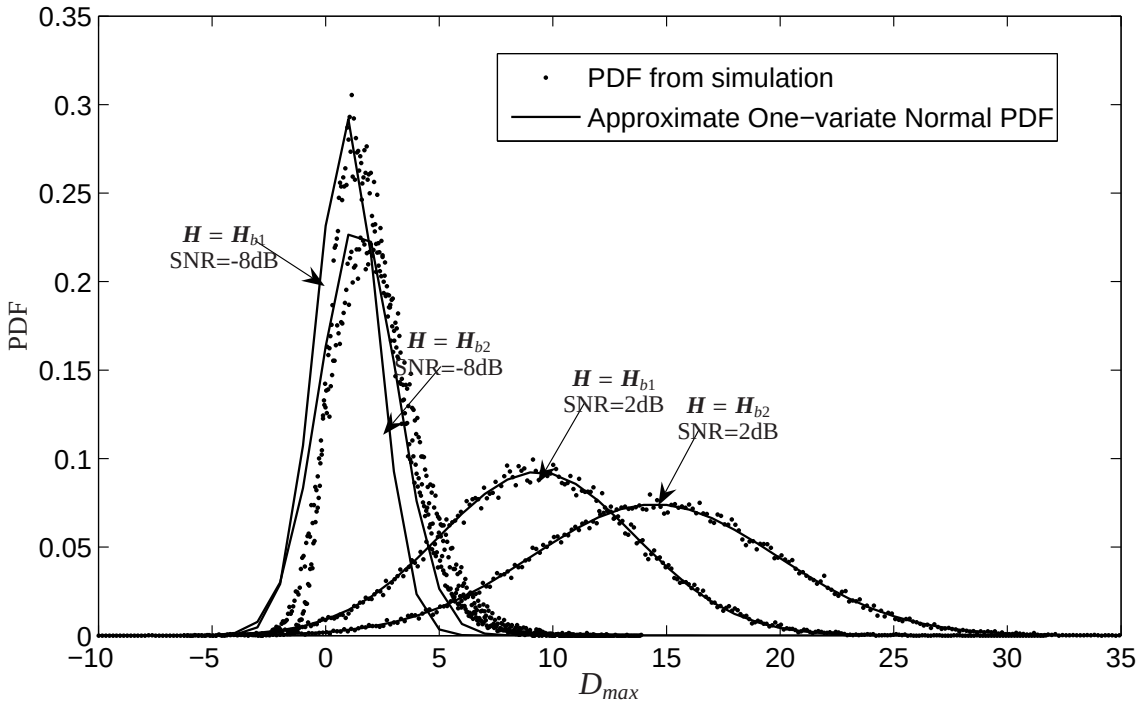



**Figure 4.3. PDFs of $D_{max}$ with $M = N = 3$.**

With lemma 4.2.3, we have the following claim on the correct detection probability.

**Lemma 4.2.4** *Given the system model in (2.3), the MLD in (4.7) and the transmitted signal* $\boldsymbol{s} = \boldsymbol{s}_u$*, we have*

$$P(\hat{\boldsymbol{s}}_{ML} = \boldsymbol{s}_u | \boldsymbol{s} = \boldsymbol{s}_u, \boldsymbol{H})$$

$$= 1 - \sum_{\boldsymbol{s}_v, v \neq u} P(\hat{\boldsymbol{s}}_{ML} = \boldsymbol{s}_v | \boldsymbol{s} = \boldsymbol{s}_u, u \neq v, \boldsymbol{H}) \tag{4.20}$$

$$\geq 1 - \sum_{\boldsymbol{s}_v, v \neq u} Q\Big(\frac{\sigma_{ML}(uv)}{2}\Big). \tag{4.21}$$

*Proof:* Plugging (4.14) in (4.20), the result is ready to obtain. □

**Remark:** For MLD, the worst case is that the noise power is infinite. Under such a condition we have

$$P(\hat{\boldsymbol{s}}_{ML} = \boldsymbol{s}_u | \boldsymbol{s} = \boldsymbol{s}_u, \boldsymbol{H}) = P(\hat{\boldsymbol{s}}_{ML} = \boldsymbol{s}_v | \boldsymbol{s} = \boldsymbol{s}_u,\ u \neq v,\ \boldsymbol{H}) = \frac{1}{|\mathcal{S}|^M}. \tag{4.22}$$

But when the noise power is constrained, the following expressions should hold:

$$P(\hat{\boldsymbol{s}}_{ML} = \boldsymbol{s}_u | \boldsymbol{s} = \boldsymbol{s}_u, \boldsymbol{H}) > P(\hat{\boldsymbol{s}}_{ML} = \boldsymbol{s}_v | \boldsymbol{s} = \boldsymbol{s}_u,\ u \neq v,\ \boldsymbol{H}), \text{ and} \tag{4.23}$$

$$P(\hat{\boldsymbol{s}}_{ML} = \boldsymbol{s}_u | \boldsymbol{s} = \boldsymbol{s}_u, \boldsymbol{H}) > \frac{1}{|\mathcal{S}|^M}, \tag{4.24}$$

which means with any finite noise power, the correct detection probability is always greater than the error probability. Therefore to make the lower bound more precisely, we adopt the lower bound only when

$$1 - \sum_{\boldsymbol{s}_v, v \neq u} Q\Big(\frac{\sigma_{ML}(uv)}{2}\Big) > Q\Big(\frac{\sigma_{ML}(uv)}{2}\Big),\ \forall v \neq u. \tag{4.25}$$

If (4.25) holds, since

$$\sum_{\boldsymbol{s}_v} P(\hat{\boldsymbol{s}}_{ML} = \boldsymbol{s}_v | \boldsymbol{s} = \boldsymbol{s}_u, \boldsymbol{H}) = 1, \tag{4.26}$$

the following inequality holds automatically:

$$1 - \sum_{\boldsymbol{s}_v, v \neq u} Q\Big(\frac{\sigma_{ML}(uv)}{2}\Big) > \frac{1}{|\mathcal{S}|^M}. \tag{4.27}$$

With the conclusions in lemma 4.2.3 and lemma 4.2.4, we present the lower bound of the PMI with MLD by employing PSK constellations.

**Theorem 4.2.5** *Given the system model in (2.3) and the MLD in (4.7), if (4.25) holds, we have*

$$\begin{aligned}
&\mathcal{I}(\boldsymbol{s}; \hat{\boldsymbol{s}}_{ML} | \boldsymbol{H}) \\
&\quad \geq M \log_2 q + \frac{1}{q^M} \sum_{\boldsymbol{s}_u} \Bigg[ \sum_{\boldsymbol{s}_v, v \neq u} Q\Big(\frac{\sigma_{ML}(uv)}{2}\Big) \log_2 Q\Big(\frac{\sigma_{ML}(uv)}{2}\Big) \\
&\qquad + \Bigg(1 - \sum_{\boldsymbol{s}_v, v \neq u} Q\Big(\frac{\sigma_{ML}(uv)}{2}\Big)\Bigg) \log_2 \Bigg(1 - \sum_{\boldsymbol{s}_v, v \neq u} Q\Big(\frac{\sigma_{ML}(uv)}{2}\Big)\Bigg)\Bigg].
\end{aligned} \tag{4.28}$$

Note that the lower bound in (4.28) also serves as an approximation of the PMI when QAM constellations are adopted.

In this section, we first derive the analytical expression of the PMI with MLD for any symbols. But it is shown that there is no closed form for the PMI. However, when PSK constellations are adopted, we propose an easily computed asymptotically tight lower bound of it, which allows us to evaluate the performance of the MIMO systems with MLD and design optimal error control codes for the systems. In the next section, we study the PMI with ZFD.

## 4.3 Post-Detection Mutual Information with Zero-Forcing Detector

Similar to the PMI with MLD, the PMI with ZFD is the mutual information between the transmitted signal $\boldsymbol{s}$ and the detected signal $\hat{\boldsymbol{s}}_{ZF}$ given by the ZFD, which is

$$\begin{aligned}
&\mathcal{I}(\boldsymbol{s}; \hat{\boldsymbol{s}}_{ZF}|\boldsymbol{H}) \\
&\quad = \mathcal{H}(\boldsymbol{s}) - \mathcal{H}(\boldsymbol{s}|\hat{\boldsymbol{s}}_{ZF}, \boldsymbol{H}) \\
&\quad = M \log_2 q + \frac{1}{q^M} \sum_{\boldsymbol{s}_v \in \mathcal{S}^M} \sum_{\boldsymbol{s}_u \in \mathcal{S}^M} \left( P(\hat{\boldsymbol{s}}_{ZF} = \boldsymbol{s}_v | \boldsymbol{s} = \boldsymbol{s}_u, \boldsymbol{H}) \log_2 \frac{P(\hat{\boldsymbol{s}}_{ZF} = \boldsymbol{s}_v | \boldsymbol{s} = \boldsymbol{s}_u, \boldsymbol{H})}{\sum_{\boldsymbol{s}_p \in \mathcal{S}^M} P(\hat{\boldsymbol{s}}_{ZF} = \boldsymbol{s}_v | \tilde{\boldsymbol{s}} = \boldsymbol{s}_p, \boldsymbol{H})} \right).
\end{aligned} \tag{4.29}$$

The PMI with ZFD is also determined by the error and the correct detection probabilities. But as shown in Section 4.2, it is difficult to get the closed form of the probabilities even with ZFD. However, the PMI with ZFD is studied as follows based on two different types of symbols, *i.e.*, PSK and QAM.

### 4.3.1 The PMI with ZFD for PSK symbols

When PSK constellations are adopted, similar to proposition 4.2.1, the PMI with ZFD for PSK symbols is given by the following proposition.

**Proposition 4.3.1** *When PSK symbols are transmitted, the PMI of a MIMO system with ZFD is given by*

$$\mathcal{I}(\boldsymbol{s};\hat{\boldsymbol{s}}_{ZF}|\boldsymbol{H}) = M\log_2 q + \frac{1}{q^M}\sum_{\boldsymbol{s}_u\in\mathcal{S}^M}\sum_{\boldsymbol{s}_v\in\mathcal{S}^M} P(\hat{\boldsymbol{s}}_{ZF}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})\log_2 P(\hat{\boldsymbol{s}}_{ZF}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H}). \tag{4.30}$$

There is still no closed form for the PMI with ZFD for PSK symbols. However, we also propose an easily computed asymptotically tight lower bound of it. But before presenting the lower bound, there are three lemmas to be given first.

**Lemma 4.3.2** *Given $\boldsymbol{s}=\boldsymbol{s}_u$, for any constellation, $\boldsymbol{s}_v$ is the detected vector with ZFD given in (4.5) if and only if*

$$(\boldsymbol{x}-\boldsymbol{s}_v)^\dagger\boldsymbol{\Lambda}(\boldsymbol{x}-\boldsymbol{s}_v) \le (\boldsymbol{x}-\boldsymbol{s}_k)^\dagger\boldsymbol{\Lambda}(\boldsymbol{x}-\boldsymbol{s}_k),\quad \forall k\neq v, \tag{4.31}$$

*where $\boldsymbol{\Lambda}$ is any diagonal matrix with all positive diagonal entries.*

With the result of Lemma 4.3.2, the error probability with ZFD is

$$\begin{aligned} P(\hat{\boldsymbol{s}}_{ZF}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,u\neq v,\boldsymbol{H}) &= P\left(\|\boldsymbol{x}-\boldsymbol{s}_v\|_{\boldsymbol{\Lambda}}^2 \le \|\boldsymbol{x}-\boldsymbol{s}_k\|_{\boldsymbol{\Lambda}}^2,\forall k\neq v\Big|\boldsymbol{s}=\boldsymbol{s}_u\right)\\ &= P\left(\max\left(\|\boldsymbol{x}-\boldsymbol{s}_v\|_{\boldsymbol{\Lambda}}^2-\|\boldsymbol{x}-\boldsymbol{s}_k\|_{\boldsymbol{\Lambda}}^2\right)\le 0,\forall k\neq v\Big|\boldsymbol{s}=\boldsymbol{s}_u\right), \end{aligned} \tag{4.32}$$

and thus the scaler minimum distance criteria of ZFD are equivalent to a minimum vector distance criterion. Similar to the case of the error probability with MLD, there is no closed form of (4.32). However, we have the following pair-wise error probability.

**Lemma 4.3.3** *Given the system model in (2.3) and the ZFD in (4.5), when $\boldsymbol{s}=\boldsymbol{s}_u$ we have*

$$P\left(\|\boldsymbol{x}-\boldsymbol{s}_v\|_{\boldsymbol{\Lambda}}^2 \le \|\boldsymbol{x}-\boldsymbol{s}_u\|_{\boldsymbol{\Lambda}}^2, u\neq v\right) = Q\Big(\frac{\mu_{ZF}(uv)}{\sigma_{ZF}(uv)}\Big), \tag{4.33}$$

*where $\mu_{ZF}(uv)$ and $\sigma_{ZF}^2(uv)$ are determined as*

$$\mu_{ZF}(uv) = \|\boldsymbol{s}_u-\boldsymbol{s}_v\|_{\boldsymbol{\Lambda}}^2 \text{ and } \sigma_{ZF}^2(uv) = 2(\boldsymbol{s}_u-\boldsymbol{s}_v)^\dagger\boldsymbol{\Lambda}\boldsymbol{W}\boldsymbol{\Lambda}(\boldsymbol{s}_u-\boldsymbol{s}_v). \tag{4.34}$$

*Proof:* The proof is similar as the proof of lemma 4.2.2.

Furthermore, we have the upper and lower bounds of the error and correct detection probabilities of ZFD, which are presented in the following lemma.

**Lemma 4.3.4** *Given the system model in (2.3) and the ZFD in (4.5), if* $\boldsymbol{s} = \boldsymbol{s}_u$*, we have*

$$P(\hat{\boldsymbol{s}}_{ZF} = \boldsymbol{s}_v | \boldsymbol{s} = \boldsymbol{s}_u, u \neq v, \boldsymbol{H}) \leq Q\Big(\frac{\mu_{ZF}(uv)}{\sigma_{ZF}(uv)}\Big), \text{ and} \tag{4.35}$$

$$P(\hat{\boldsymbol{s}}_{ZF} = \boldsymbol{s}_u | \boldsymbol{s} = \boldsymbol{s}_u, \boldsymbol{H}) \geq 1 - \sum_{\boldsymbol{s}_v, v \neq u} Q\Big(\frac{\mu_{ZF}(uv)}{\sigma_{ZF}(uv)}\Big), \tag{4.36}$$

*where* $\mu_{ZF}(uv)$ *and* $\sigma_{ZF}(uv)$ *are given in (4.34) and* $\boldsymbol{\Lambda}$ *in (4.34) is any non-identity diagonal matrix with all positive diagonal entries.*

**Remark:** To make Lemma 4.3.4 valid, there is one thing to emphasize that $\boldsymbol{\Lambda}$ cannot be identity matrix. The reason for that is if $\boldsymbol{\Lambda} = \boldsymbol{I}_M$ then $\|\boldsymbol{s} - \boldsymbol{s}_v\|^2_{\boldsymbol{\Lambda}} = \|\boldsymbol{s} - \boldsymbol{s}_v\|^2$ cannot be randomized weighted on different entries of $\boldsymbol{s} - \boldsymbol{s}_v$. Thus, the distribution of $\max\Big(\|\boldsymbol{x} - \boldsymbol{s}_v\|^2_{\boldsymbol{\Lambda}} - \|\boldsymbol{x} - \boldsymbol{s}_k\|^2_{\boldsymbol{\Lambda}} | \boldsymbol{s} = \boldsymbol{s}_u, \forall k \neq v\Big)$ is no longer Gaussian-like.

Now we are ready to present the lower bound of the PMI with ZFD when PSK symbols are transmitted.

**Theorem 4.3.5** *Given the system model in (2.3) and the ZFD in (4.5), we have*

$$\begin{aligned} \mathcal{I}(\boldsymbol{s}; \hat{\boldsymbol{s}}_{ZF} | \boldsymbol{H}) \geq M \log_2 q + \frac{1}{q^M} \sum_{\boldsymbol{s}_u} \Bigg[ \sum_{\boldsymbol{s}_v, v \neq u} Q\Big(\frac{\mu_{ZF}(uv)}{\sigma_{ZF}(uv)}\Big) \log_2 Q\Big(\frac{\mu_{ZF}(uv)}{\sigma_{ZF}(uv)}\Big) \\ + \Bigg(1 - \sum_{\boldsymbol{s}_u, u \neq v} Q\Big(\frac{\mu_{ZF}(uv)}{\sigma_{ZF}(uv)}\Big)\Bigg) \log_2 \Bigg(1 - \sum_{\boldsymbol{s}_u, u \neq v} Q\Big(\frac{\mu_{ZF}(uv)}{\sigma_{ZF}(uv)}\Big)\Bigg)\Bigg]. \end{aligned} \tag{4.37}$$

*Proof:* The proof is similar to the proof of Theorem 4.2.5.

Theorem 4.3.5 provides a lower bound for the PMI with ZFD for PSK symbols. When the transmitted symbols are QAM symbols, the exact value of the PMI with ZFD can be numerically computed.

### 4.3.2 The PMI with ZFD for QAM symbols

When QAM symbols are transmitted, neither Theorem 4.2.5 nor Theorem 4.3.5 holds any longer. However, we observe that the error and the correct detection probabilities are still

needed to compute the PMI with ZFD. Actually, both the error and the correct detection probabilities can be computed by integrating the *probability density function* (PDF) of the equalized signal $\boldsymbol{x}$ over the corresponding decision cells. For example, the error probability is

$$P(\hat{\boldsymbol{s}}_{ZF} = \boldsymbol{s}_v | \boldsymbol{s} = \boldsymbol{s}_u, \boldsymbol{H}) = \int_{\Omega_{\hat{\boldsymbol{s}}_{ZF}=\boldsymbol{s}_v}} \boldsymbol{x} d\boldsymbol{x}, \tag{4.38}$$

where $\Omega_{\hat{\boldsymbol{s}}_{ZF}=\boldsymbol{s}_v}$ is the decision cell for $\hat{\boldsymbol{s}}_{ZF} = \boldsymbol{s}_v$. For instance, in a $2 \times 2$ MIMO system, when 4-QAM symbols are applied, the decision cell for $\hat{\boldsymbol{s}}_{ZF} = [1+i \quad 1+i]^T$ is $\Omega_{\hat{\boldsymbol{s}}_{ZF}=\boldsymbol{s}_v} = \{x1, x2 : Re\{x_1\} > 0,\ Im\{x_1\} > 0,\ Re\{x_2\} > 0, \text{ and } Im\{x_4\} > 0\}$. The coordinates of the edge points of the decision cell are $[0\ 0\ 0\ 0]^T$ and $[+\infty\ +\infty\ +\infty\ +\infty]^T$.

Let

$$\boldsymbol{z} = \begin{bmatrix} Re\{\boldsymbol{x}\} \\ Im\{\boldsymbol{x}\} \end{bmatrix}, \tag{4.39}$$

where $\boldsymbol{z}$ is a $2M \times 1$ vector and the joint distribution of all the entries of $\boldsymbol{z}$ is known to be multivariate Gaussian distributed. Therefore, the integral in (4.38) is a multivariate Gaussian integral over $\Omega_{\hat{\boldsymbol{s}}_{ZF}=\boldsymbol{s}_v}$ [71–73]. In fact, the multivariate Gaussian integral over any cell is still an unsolved problem. But notice that for any QAM symbols, the coordinates of the edge points of the decision cells given by ZFD are all constant. With the constant coordinates of the edge points, the integral in (4.38) can be decomposed into multiple one-variate normal integrals. The decomposition of the integral in (4.38) offers a foundation to numerically calculate the PMI with ZFD. The details are given in the following.

First, we need to find the covariance matrix of $\boldsymbol{z}$, which is defined as

$$\boldsymbol{\Sigma} = E[\boldsymbol{z}\boldsymbol{z}^T]. \tag{4.40}$$

**Lemma 4.3.6** *Given the equalized vector $\boldsymbol{x}$ in (4.3), the covariance matrix $\boldsymbol{\Sigma}$ defined in*

*(4.40) can be calculated as*

$$\boldsymbol{\Sigma} = \sigma_\omega^2 \begin{bmatrix} \boldsymbol{A} & -\boldsymbol{B} \\ \boldsymbol{B} & \boldsymbol{A} \end{bmatrix} \begin{bmatrix} \boldsymbol{A}^T & \boldsymbol{B}^T \\ -\boldsymbol{B}^T & \boldsymbol{A}^T \end{bmatrix} \tag{4.41}$$

$$= \sigma_\omega^2 \begin{bmatrix} \boldsymbol{A}\boldsymbol{A}^T + \boldsymbol{B}\boldsymbol{B}^T & \boldsymbol{A}\boldsymbol{B}^T - \boldsymbol{B}\boldsymbol{A}^T \\ \boldsymbol{B}\boldsymbol{A}^T - \boldsymbol{A}\boldsymbol{B}^T & \boldsymbol{A}\boldsymbol{A}^T + \boldsymbol{B}\boldsymbol{B}^T \end{bmatrix} \tag{4.42}$$

*where* $\boldsymbol{A} = Re\{\boldsymbol{H}^\dagger\}$ *and* $\boldsymbol{B} = Im\{\boldsymbol{H}^\dagger\}$.

Now the joint PDF of $\boldsymbol{z}$ given $\boldsymbol{s} = \boldsymbol{s}_u$ can be expressed by

$$f(\boldsymbol{z}|\boldsymbol{s} = \boldsymbol{s}_u) = \frac{1}{\sqrt{(2\pi)^{2M}\det(\boldsymbol{\Sigma})}} exp\left[-\frac{1}{2}(\boldsymbol{z} - \boldsymbol{\upsilon})^T \boldsymbol{\Sigma}^{-1}(\boldsymbol{z} - \boldsymbol{\upsilon})\right], \tag{4.43}$$

where $\boldsymbol{\upsilon} = [Re\{\boldsymbol{s}_u^T\}\ Im\{\boldsymbol{s}_u^T\}]^T$. Based on (4.43) we have

$$\begin{aligned} P(\hat{\boldsymbol{s}}_{ZF} = \boldsymbol{s}_v|\boldsymbol{s} = \boldsymbol{s}_u, \boldsymbol{H}) &= \int_{\Omega_{\hat{\boldsymbol{s}}_{ZF}=\boldsymbol{s}_v}} \boldsymbol{x}d\boldsymbol{x} \\ &= \frac{1}{\sqrt{(2\pi)^{2M}\det(\boldsymbol{\Sigma})}} \int_{a_{\boldsymbol{s}_v,1}}^{b_{\boldsymbol{s}_v,1}} \int_{a_{\boldsymbol{s}_v,2}}^{b_{\boldsymbol{s}_v,2}} \cdots \int_{a_{\boldsymbol{s}_v,2M}}^{b_{\boldsymbol{s}_v,2M}} exp\{-\frac{1}{2}(\boldsymbol{z} - \boldsymbol{\upsilon})^T \boldsymbol{\Sigma}^{-1}(\boldsymbol{z} - \boldsymbol{\upsilon})\} d\boldsymbol{z} \\ &= \frac{1}{\sqrt{(2\pi)^{2M}\det(\boldsymbol{\Sigma})}} \int_{c_{\boldsymbol{s}_v,1}}^{d_{\boldsymbol{s}_v,1}} \int_{c_{\boldsymbol{s}_v,2}}^{d_{\boldsymbol{s}_v,2}} \cdots \int_{c_{\boldsymbol{s}_v,2M}}^{d_{\boldsymbol{s}_v,2M}} exp\{-\frac{1}{2}(\boldsymbol{z}')^T \boldsymbol{\Sigma}^{-1}\boldsymbol{z}'\} d\boldsymbol{z}' \\ &= F(\boldsymbol{s}_u, \boldsymbol{s}_v, \boldsymbol{\Sigma}) \end{aligned} \tag{4.44}$$

where $a_{\boldsymbol{s}_v,k}$ and $b_{\boldsymbol{s}_v,k}$, for $k = 1, \cdots, 2M$, denote the lower and higher boundaries of the $k$-th domain of $\Omega_{\hat{\boldsymbol{s}}_{ZF}=\boldsymbol{s}_v}$,

$$c_{\boldsymbol{s}_v,k} = a_{\boldsymbol{s}_v,k} - \upsilon_k \ \text{ and } \ d_{\boldsymbol{s}_v,k} = b_{\boldsymbol{s}_v,k} - \upsilon_k. \tag{4.45}$$

For example, with 4-QAM constellation, if $\hat{\boldsymbol{s}}_{ZF} = \boldsymbol{s}_1 = [1+i \quad 1+i]^T$ and $\boldsymbol{s} = \boldsymbol{s}_3 = [1-i \quad 1-i]^T$, then $\boldsymbol{\upsilon} = [1\ 1\ \ -1\ \ -1]$, $a_{\boldsymbol{s}_1,k} = 0$ and $b_{\boldsymbol{s}_1,k} = +\infty$, for $k = 1, 2, \cdots 4$. By (4.45), $c_{\boldsymbol{s}_1,1} = c_{\boldsymbol{s}_1,2} = 0 - 1 = -1$, $c_{\boldsymbol{s}_1,3} = c_{\boldsymbol{s}_1,4} = 0 - (-1) = 1$ and $d_{\boldsymbol{s}_1,k} = +\infty$, for $k = 1, 2, \cdots 4$. As we discussed at the beginning of this section, $a_{\boldsymbol{s}_v,k}$, $b_{\boldsymbol{s}_v,k}$, $c_{\boldsymbol{s}_v,k}$ and $d_{\boldsymbol{s}_v,k}$ are constant for $k = 1, 2, \cdots 2M$ once the constellation is known.

Now let us work on the multivariate Gaussian integral in (4.44). Actually, the computation of multivariate normal probability is a widely attractive problem. The pioneer research

work on it began in the 1960s. With the development of engineering techniques, people have become more and more interested in it. Unfortunately, by now, only a few special cases can be worked out. The calculation of $F(\boldsymbol{s}_u, \boldsymbol{s}_v, \boldsymbol{\Sigma})$ defined in (4.44) is one of the special cases that has constant integral limits. We adopt the method presented in [74] to compute the integral. Since $\boldsymbol{\Sigma}$ is a covariance matrix, it is symmetric and semi-definite and it has Choleskey decomposition. Let $\boldsymbol{\Sigma} = \boldsymbol{L}\boldsymbol{L}^T$, where $\boldsymbol{L}$ is a lower-triangular matrix with the $(m, n)$th entry $L_{m,n}$ calculated as

$$L_{m,n} = \begin{cases} \sqrt{\Sigma_{n,n} - \sum_{k=1}^{n-1} L_{n,k}^2} & \text{if } m = n \\ \frac{1}{L_{m,n}} \left( \Sigma_{m,n} - \sum_{k=1}^{n-1} L_{m,k} L_{n,k} \right) & \text{if } m > n. \end{cases} \tag{4.46}$$

After some transformation we have

$$\boldsymbol{z'}^T \boldsymbol{\Sigma}^{-1} \boldsymbol{z'} = \boldsymbol{z'}^T \boldsymbol{L}^{-T} \boldsymbol{L}^{-1} \boldsymbol{z'} = \boldsymbol{\varphi}^T \boldsymbol{\varphi} \tag{4.47}$$

where $\boldsymbol{\varphi} = \boldsymbol{L}^{-1} \boldsymbol{z'}$. Substituting (4.47) in (4.44), $F(\boldsymbol{s}_u, \boldsymbol{s}_v, \boldsymbol{\Sigma})$ can be decomposed into multiple integrals as

$$F(\boldsymbol{s}_u, \boldsymbol{s}_v, \boldsymbol{\Sigma}) = \frac{1}{\sqrt{(2\pi)^{2M}}} \int_{c'_{\boldsymbol{s}_v,1}}^{d'_{\boldsymbol{s}_v,1}} e^{-\frac{\varphi_1^2}{2}} \int_{c'_{\boldsymbol{s}_v,2}(\varphi_1)}^{d'_{\boldsymbol{s}_v,2}(\varphi_1)} e^{-\frac{\varphi_2^2}{2}} \cdots \int_{c'_{\boldsymbol{s}_v,2M}(\varphi_1,\cdots,\varphi_{2M-1})}^{d'_{\boldsymbol{s}_v,2}(\varphi_1,\cdots,\varphi_{2M-1})} e^{-\frac{\varphi_{2M}^2}{2}} d\boldsymbol{\varphi}, \tag{4.48}$$

where

$$c'_{\boldsymbol{s}_v,k}(\varphi_1, \cdots, \varphi_{k-1}) = \left( c_{\boldsymbol{s}_v,k} - \sum_{p=1}^{k-1} L_{k,p} \varphi_p \right) / L_{k,k} \tag{4.49}$$

and

$$d'_{\boldsymbol{s}_v,k}(\varphi_1, \cdots, \varphi_{m-1}) = (d_{\boldsymbol{s}_v,k} - \sum_{p=1}^{k-1} L_{k,p} \varphi_p) / L_{k,k}. \tag{4.50}$$

Based on (4.48), $F(\boldsymbol{s}_u, \boldsymbol{s}_v, \boldsymbol{\Sigma})$ can be numerically calculated. The details are given in [74]. Now we are ready to present the following theorem, which gives the answer to the PMI with ZFD for QAM symbols.

**Theorem 4.3.7** *When QAM constellations are employed, the PMI with ZFD in (4.30) is*

$$\mathcal{I}(\boldsymbol{s};\hat{\boldsymbol{s}}_{ZF}|\boldsymbol{H}) = M\log_2 q + \frac{1}{q^M}\sum_{\boldsymbol{s}_v\in\mathcal{S}^M}\sum_{\boldsymbol{s}_u\in\mathcal{S}^M}\left(F(\boldsymbol{s}_u,\boldsymbol{s}_v,\boldsymbol{\Sigma})\log_2\frac{F(\boldsymbol{s}_u,\boldsymbol{s}_v,\boldsymbol{\Sigma})}{\sum\limits_{\boldsymbol{s}_p\in\mathcal{S}^M}F(\boldsymbol{s}_p,\boldsymbol{s}_v,\boldsymbol{\Sigma})}\right), \tag{4.51}$$

*where* $F(\boldsymbol{s}_p,\boldsymbol{s}_v,\boldsymbol{\Sigma})$ *is given in (4.48)-(4.50).*

*Proof:* Plugging (4.44) in (4.30), (4.51) is obtained. □

Now we give some remarks on when QAM constellation is adopted, and why the exact numerical calculation of the PMI with ZFD can be carried out but MLD can not. The reason is the nature characteristics of MLD and ZFD themselves. From (4.5) and (4.7), we can see that the preliminary difference between the ZFD and MLD is the way they quantify the equalized vector $\boldsymbol{x}$. ZFD quantifies $\boldsymbol{x}$ symbol by symbol. As discussed before, the coordinates of the edge points of the decision cells are always constant when a QAM constellation is employed. Thus the integral in (4.44) can be decomposed into multiple one-variate normal integrals. But the situation is totally different for MLD. For MLD we have

$$P(\hat{\boldsymbol{s}}_{ML} = \boldsymbol{s}_v|\boldsymbol{s} = \boldsymbol{s}_u, \boldsymbol{H}) = \int_{\Omega_{\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v}} \boldsymbol{x}d\boldsymbol{x}, \tag{4.52}$$

where $\Omega_{\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v}$ is the decision cell for $\hat{\boldsymbol{s}}_{ML} = \boldsymbol{s}_v$. Different from ZFD, the coordinates of the edge points of the decision cell $\Omega_{\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v}$ are the solutions of

$$\|\boldsymbol{x}-\boldsymbol{s}_v\|^2_{\boldsymbol{W}^{-1}} = \|\boldsymbol{x}-\boldsymbol{s}_u\|^2_{\boldsymbol{W}^{-1}}, \forall \boldsymbol{s}_u \in \mathcal{S}^M \text{and } u \neq v. \tag{4.53}$$

It is obvious from (4.53), that when the covariance matrix $\boldsymbol{W}$ is not a diagonal matrix, the coordinates are not constant any more. Instead they are some variables satisfying (4.53). First of all, it is very hard to calculate the solutions of (4.53). Even if they are calculated, we still need to do multivariate Gaussian integral over $\Omega_{\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v}$ to get the PMI with MLD. Unfortunately, the multivariate Gaussian integral with any integral cell is still an unsolved problem in mathematics. Therefore, the PMI with MLD cannot be numerically computed.

## 4.4 Relationship between PMI with MLD and PMI with ZFD

When the transmitted symbols are from PSK constellations, we have presented the lower bounds of the PMI with MLD and ZFD. When QAM constellations are applied, the exact numerical computation of the PMI with ZFD is also presented. Now let us try to find out the underling fundamental parameter that brings the difference between the PMI with MLD and ZFD. Actually, when a Gaussian symbol is applied, Ma and Zhang [28] show that the orthogonality deficiency of the channel matrix $\boldsymbol{H}$, which is denoted by $od(\boldsymbol{H})$, is the parameter that directly affects the difference between the channel capacities with MLE and ZFE. The question is what happens with MLD and ZFD. In the following we give a partial answer to this question.

**Theorem 4.4.1** *Given the system model in (2.3), if* $od(\boldsymbol{H}) = 0$*, we have*

$$\mathcal{I}(\boldsymbol{s}; \hat{\boldsymbol{s}}_{ML}|\boldsymbol{H}) = \mathcal{I}(\boldsymbol{s}; \hat{\boldsymbol{s}}_{ZF}|\boldsymbol{H}), \tag{4.54}$$

*where* $od(\boldsymbol{H})$ *is the orthogonal deficiency of* $\boldsymbol{H}$ *and is defined by [28]*

$$od(\boldsymbol{H}) = 1 - \frac{\det(\boldsymbol{H}^{\mathcal{H}}\boldsymbol{H})}{\prod_{m=1}^{M} \|\boldsymbol{h}_m\|^2}, \tag{4.55}$$

*and* $\boldsymbol{h}_m$ *is the m-th column of* $\boldsymbol{H}$.

## 4.5 Numerical Results

Simulation results are presented to verify the conclusions claimed in this paper. The channel model is given in (2.3) and the channel matrix is complex Gaussian distributed. A 4-PSK (which is the same as 4-QAM) constellation is adopted as the modulation type.

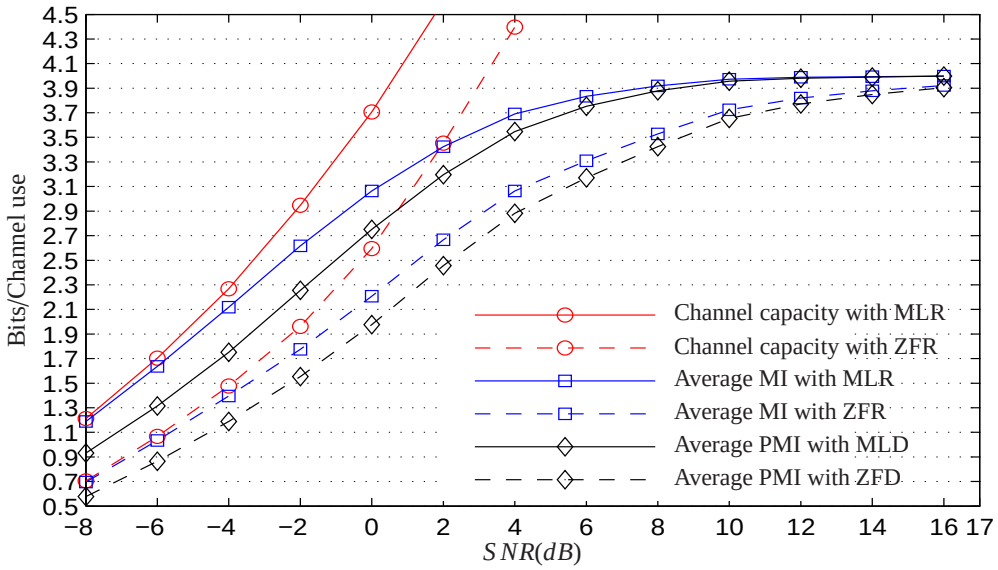
First, we compare the average and outage mutual information with different system models. Figure 4.4(a) shows the average channel capacities, the average MI with MLR or ZFR, and the average PMI with MLD or ZFD. When the input is allowed to be continuous, channel capacities with both MLR and ZFR increase monotonically as SNR increases and there is no constraint for them. When the input symbols are 4-PSK symbols, the MI with

MLR or ZFR and the PMI with MLD or ZFD are obtained from Monte Carlo simulations. The channels are $2 \times 2$ complex Gaussian distributed. Verified by Figure 4.4(a), the quantization in MLD or ZFD does reduce the MI compared with the MI without quantization. When SNR is below $6dB$, the difference is around 0.2 bits/channel use. Figure 4.4(b) shows the outage results. The outage MI is defined by

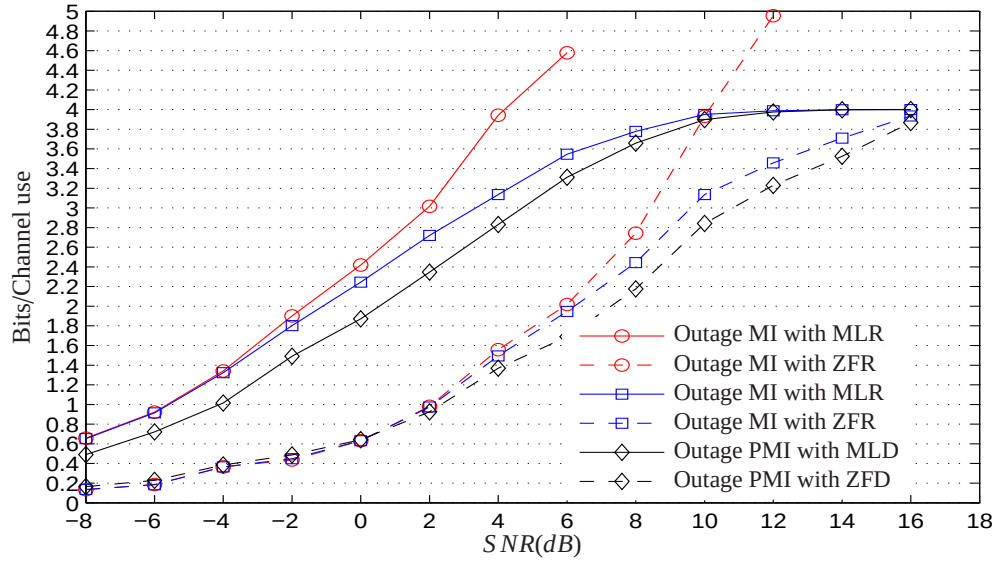
$$P\{\mathcal{I}(\boldsymbol{H}) < \mathcal{I}_{out}\} = \varepsilon. \tag{4.56}$$

In Figure 4.4(b), $\varepsilon = 0.1$. As shown in Figure 4.4(b), when SNR is below $4dB$ the difference between the MI with MLR and MLD is about 0.4 bits/channel use. The outage results verify the reduction induced by the quantization again.

Next we examine how well the lower bounds proposed in this proposal match the simulated results obtained from Monte Carlo simulations. In Figure 4.5(a), we plot the average PMI with MLD or ZFD from the simulation and the lower bounds of the PMI given in Theorem 4.2.5 and 4.3.5. From Figure 4.5(a), we observe that when SNR is larger than $4dB$, the difference between the average PMI and its lower bound proposed in Theorems 4.2.5 and 4.3.5 is less than 0.2 bits/channel use. When SNR is higher, the difference between the curves from the simulation and the curves obtained from Theorem 4.2.5 and 4.3.5 are smaller. As we proposed in Theorem 4.3.7, when QAM constellations are adopted, the PMI with ZFD can be exactly numerically computed by (4.51). As shown in Figure 4.5(a), the results obtained by (4.51) match exactly with the results from Monte Carlo simulations. In Figure 4.5(b), we plot the outage results with $\varepsilon = 0.1$. Similar conclusions can be drawn from the outage results in Figure 4.5(b).

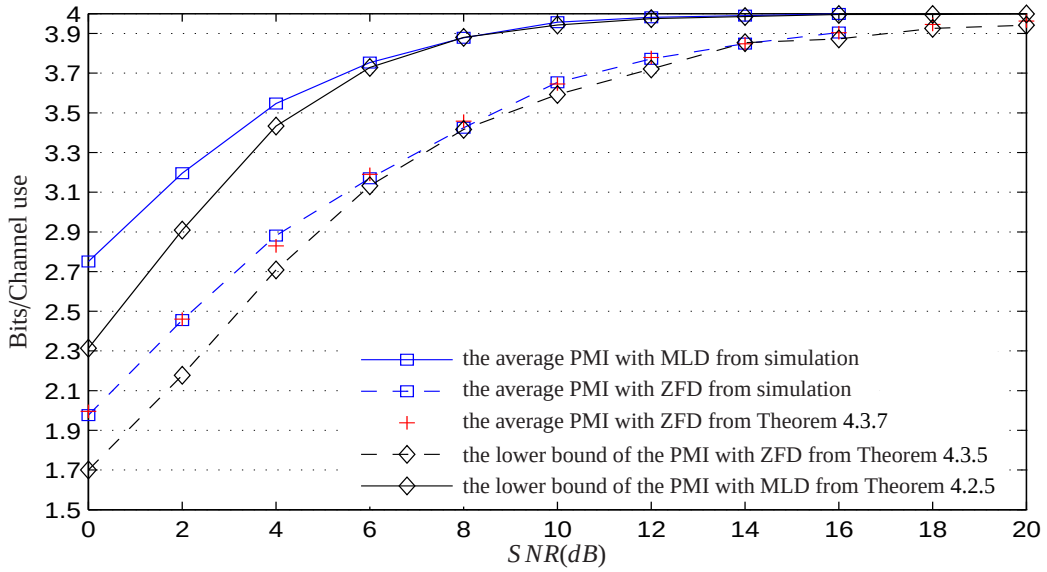



(a) Average results.

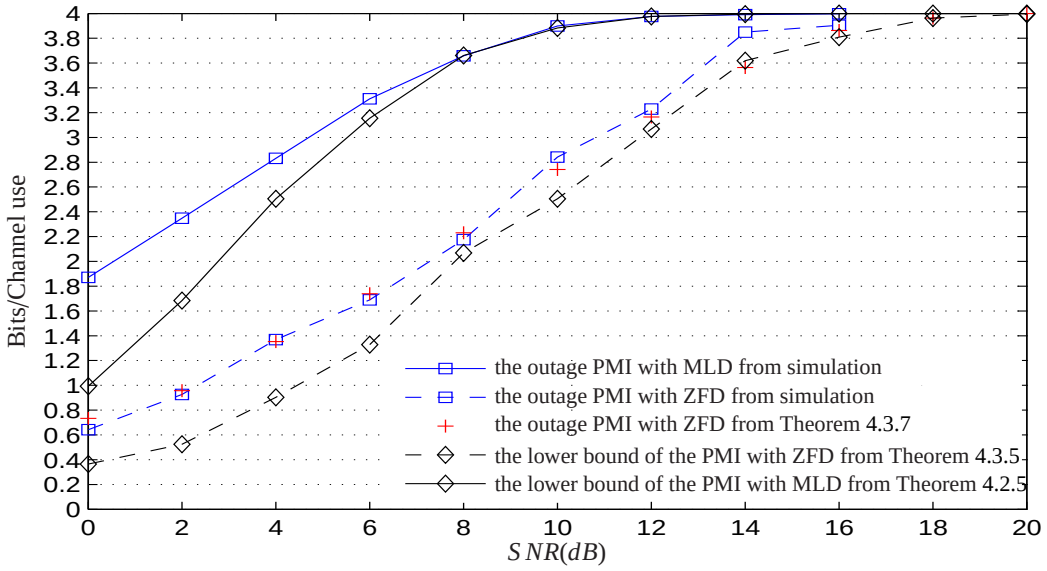



(b) Outage results with $\varepsilon = 0.1$.

**Figure 4.4. Channel capacities with MLR and ZFR, MI with MLR and ZFR for 4-PSK and the PMI with MLD and ZFD for 4-PSK,** $M = N = 2$**.**




(a) Average results.




(b) Outage results.

**Figure 4.5. Simulated PMI and the lower bounds of PMI with MLD and ZFD for 4-PSK and $M = N = 2$.**

## 4.6 Conclusion

This is the first time to study the influence of quantization on the mutual information for communications. First of all, we derive the analytical expression of the PMI with MLD or ZFD. Then the easily computed asymptotically lower bounds of them are proposed for PSK constellations. The lower bounds also serve as the approximations when QAM constellations are adopted. Furthermore, when QAM constellations are adopted, we provide the closed form of the PMI with ZFD. The values obtained from the closed formula match exactly the results from the simulations. We have also shown that when $od(\boldsymbol{H}) = 0$, the PMI with MLD or ZFD is equal to each other which is consistent with the case for the MI with ML and ZF receiver. Finally the numerical results show that hard detection does reduce the MI.

# CHAPTER 5

# RANDOM COMPLEX FIELD CODE DESIGN FOR SECURITY OVER WIRETAP CHANNELS

Security has become one of the main concerns for communications. Among all malicious attacks, eavesdropping is a large class and quite common for wireless transmissions. Wyner's wiretap channel setup fits eavesdropping scenario where the communication between the sender and the legitimate receiver can be seen as the main channel and the other traffic to eavesdropper is seen as the wiretapper's channel. Wyner and later Csiszár and Körner prove that when the secrecy rate is below the secrecy capacity, there should exist channel codes, which can guarantee both robustness to transmission errors to the legitimate receiver and a prescribed degree of data confidentiality for the eavesdropper. Hence the wiretap channel setup can be applied in communications to achieve the security in physical layer. A fundamental and well adopted wiretap channel model is that the main channel is noiseless and the eavesdroppers' channel is *binary erasure channel* (BEC). LDPC codes have been applied to achieve secrecy capacity of such wiretap channels. However, it lacks design flexibility and cannot illustrate the fundamental tradeoffs among the secrecy rate, erasure rate, and the secrecy performance. In this chapter, we present a *random complex field code* (RCFC) design for such wiretap channels. The design of RCFCs is systematic and flexible for any code rate. Our analysis shows that RCFC can achieve the secrecy capacity as the code length goes to infinity. More strikingly, the presented design is the first one which provides a platform to tradeoff secrecy performance with the erasure rate of the eavesdropper's channel and the secrecy rate.

The rest of the chapter is organized as follows. In Section 5.1, we describe the wiretap channel discussed in the chapter. The design of RCFC is presented in the following Section 5.2. Section 5.3 describes the decoding strategies of Eve. In Section 5.4, we analyze the

security performance of RCFC and provide a way to design RCFC with desired performance. The decoding complexity for both Bob and Eve are studied in Section 5.5. Section 5.6 presents numerical results which verify the performance of RCFC. Finally, Section 5.7 concludes the chapter.

## 5.1 Wiretap Channel

In 1975, Wyner introduced another scenario of communication with information-theoretic security [31]. In his seminal work, the wiretap channel is introduced, which is depicted in Fig. 5.1. In a wiretap channel, Alice wants to transmit confidential messages $\boldsymbol{s}$ to the legitimate receiver Bob through a *discrete memoryless channel* (DMC) C1, whereas an eavesdropper Eve may receive partially the transmitted message through another different DMC C2. We call C1 as the main channel and C2 as the wiretapper's channel. To secure the message $\boldsymbol{s}$, Alice encodes $m$-symbol message $\boldsymbol{s}$ into a $n$-symbol codeword $\boldsymbol{x}$ and then transmits $\boldsymbol{x}$. The observations at Bob and Eve are denoted by $\boldsymbol{y}$ and $\boldsymbol{z}$, respectively. There are two objectives to be achieved simultaneously by Alice's encoder: **reliability** and **security**. More specifically, reliability requires that the legitimate receiver Bob should decode $\boldsymbol{s}$ based on its observation $\boldsymbol{y}$ with negligible small error probability; while security requires that Eve has no knowledge about $\boldsymbol{s}$ via its own observation $\boldsymbol{z}$ when the codeword length $n$ goes to infinity, i.e., $\frac{1}{n}\mathcal{I}(\boldsymbol{s}, \boldsymbol{z}) \to 0$ as $n \to \infty$. Wyner has shown that when C2 is a "degraded" version of C1 (either physically or statistically), Alice can securely transmit the message at a positive rate $m/n$ [31], which means both the reliable and secure communications can be achieved. The rate $m/n$ is called the secrecy rate. The maximum value of the possible secrecy rate is characterized by Wyner as the secrecy capacity $C_s$ [31]. Csiszár and Körner extended the result to general wiretap channels [75]. More results on the security capacity of other broadcast channel scenarios can be found in [76–78]. To realize the secure and reliable communication in a wiretap channel model, i.e., the security capacity is strictly positive, the main channel must have some advantage over the wiretapper's

channel. But, more recently, Maurer proved that even the channel between Alice and Bob is worse than the channel between Alice and Eve, it is still possible to generate a secret key by public discussion [79]. However, in this chapter, since we do not allow interactive communication between Alice and Bob, we focus on wiretap channel with strictly positive secrecy capacity.

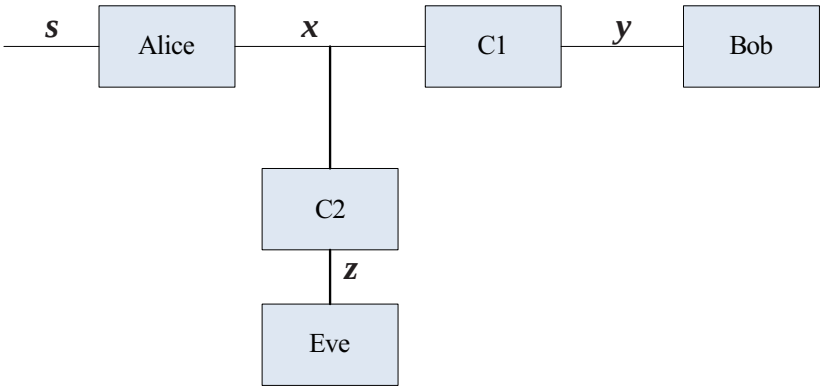



**Figure 5.1. Wiretap channel model.**

Wyner and later Csiszár and Körner proved that when the secrecy rate is below the secrecy capacity, there should exist a coding scheme to achieve both reliable and secure transmission simultaneously [31, 75]. Unfortunately, how to design the effective codes for a wiretap channel is still an open problem. So far, the most widely-adopted technique is low-density parity-check (LDPC) codes proposed in [32, 80, 81]. It was shown in [32, 82] and [81] that LDPC codes can asymptotically approach the secrecy capacity.

In this chapter, we consider the same channel model as in [32] where the main channel is noiseless and the wiretapper's channel is BEC. We propose a non-binary design for such a wiretap channel by using RCFC technique. The main idea for *RCFC is to mix some random symbols with the information symbols so that Eve can decode them with extremely low probability but Bob still can decode them correctly*. The RCF codes are easy to design with any given code rates. We show that when the erasure rate of BEC is greater than zero, RCFC can achieve the secrecy capacity asymptotically. Moreover, when the secrecy rates are below the secrecy capacity, RCFC can realize perfectly secure communication,

i.e., both reliability and security can be achieved simultaneously. More important, not only do we prove that RCFC is secrecy capacity-achieving codes, but also we can illustrate the fundamental tradeoffs among the secrecy rate, erasure rate, and the lower bound of the normalized security information rate, which is a metric of how secure the coding scheme is. Hence, the RCFC can be designed as required by the users or the providers. However, there are no such tradeoffs available for LDPC codes.

## 5.2 Random Complex Field Code

In this section, we describe the encoding scheme of RCF codes. As depicted in Fig. 5.2, there are two steps to encode the confidential message $\boldsymbol{s}$. The first step is to form a codeword matrix $\Gamma$. The second one is performing *linear complex field* (LCF) symbol mixing. In the first step, the codeword matrix is formed of three kinds of symbols, *i.e.*, the confidential information symbols $\boldsymbol{s}$, the random symbols $u_{p,q}$ and the check symbols. The $m \times 1$ confidential symbol vector contains complex symbols $s_p$ which are uniformly randomly drawn from a QAM constellation $\mathcal{S}$. The size of the constellation $\mathcal{S}$ is $M$. The random symbols $u_{p,q}$ are also randomly chosen from $\mathcal{S}$ (the same as the one for $s_p$).

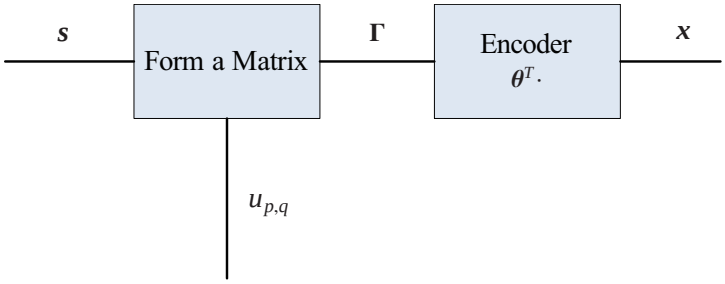



**Figure 5.2. LCF encoding scheme.**

The $m \times n$ codeword matrix $\mathbf{\Gamma}$ is constructed as follows:

1) information symbols $s_p$ is put in the $p$-th row of $\mathbf{\Gamma}$, but any column of $\mathbf{\Gamma}$ with equal probability;

2) random symbol $u_{p,q}$ for $p = 1, \cdots, m,\ q = 1, \cdots, n-2$, is randomly drawn from $\mathcal{S}$ and placed at the $p$th row randomly;

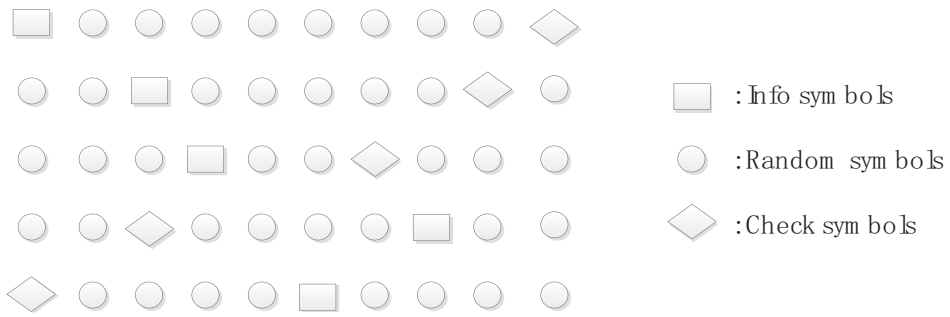



**Figure 5.3. Elements of $\Gamma$.**

3) check symbol $c_p$ is placed at the $p$th row of $\mathbf{\Gamma}$ with the value equal to

$$c_p = -\sum_{q=1,\cdots,n} u_{p,q}. \tag{5.1}$$

Figure 5.3 illustrates the structure of the codeword matrix $\Gamma$.

From the codeword matrix construction, we observe that every row of $\mathbf{\Gamma}$ contains one information symbol, $n-2$ random symbols, and one check symbol and it contains high uncertainty due to the mixed random symbols and unknown placements. Note that the legitimate receiver Bob does not know the random symbols and check symbols. To guarantee that Bob can still decode the information symbols, we need the following operation.

The codeword matrix $\mathbf{\Gamma}$ is further compressed into a vector by a linear CF encoder. The encoding matrix $\boldsymbol{\theta}$ is an $m \times 1$ complex vector with well designed structure which ensures that there is a one-to-one mapping between $\boldsymbol{\theta}^T \mathbf{r}$ and $\mathbf{r}$ if $r_p$ (the $p$-th element of $\mathbf{r}$) for $p = 1, \cdots, m$ is a QAM symbol. Here we adopt the first row of the linear precoding matrix in [83, 84] as $\boldsymbol{\theta}^T$. In other words, once the value of $\boldsymbol{\theta}^T \mathbf{r}$ is given, then $\mathbf{r}$ can be uniquely identified.

**Example 2:** *when $m = 2$, according to the design criteria in [83, 84], we have*

$$\boldsymbol{\theta}^T = [1 \; e^{j\frac{\pi}{8}}] \tag{5.2}$$

*where $\alpha = e^{j\frac{\pi}{8}}$. When 4-QAM constellation is used ($\mathcal{S} = \{1+j \; -1+j \; -1-j \; 1-j\}$), the one-to-one mapping table between the possible $\mathbf{r}$ and $\boldsymbol{\theta}^T \mathbf{r}$ is given in Table 5.1.*

**Table 5.1. Mapping table between $\boldsymbol{r}$ and $\boldsymbol{\theta}^T\boldsymbol{r}$**

| $\boldsymbol{r}$ | $\boldsymbol{\theta}^T\boldsymbol{r}$ |
|---|---|
| $[-1+j,\ -1+j]^T$ | $-2.3066+1.5412j$ |
| $[-1+j,\ -1-j]^T$ | $-1.5412-0.3066j$ |
| $[-1+j,\ 1+j]^T$ | $-0.4588+2.3066j$ |
| $[-1+j,\ 1-j]^T$ | $0.3066+0.4588j$ |
| $[-1-j,\ -1+j]^T$ | $-2.3066-0.4588j$ |
| $[-1-j,\ -1-j]^T$ | $-1.5412-2.3066j$ |
| $[-1-j,\ 1+j]^T$ | $-0.4588+0.3066j$ |
| $[-1-j,\ 1-j]^T$ | $0.3066-1.5412j$ |
| $[1+j,\ -1+j]^T$ | $-0.3066+1.5412j$ |
| $[1+j,\ -1-j]^T$ | $0.4588-0.3066j$ |
| $[1+j,\ 1+j]^T$ | $1.5412+2.3066j$ |
| $[1-j,\ -1-j]^T$ | $2.3066+0.4588j$ |
| $[1-j,\ -1+j]^T$ | $-0.3066-0.4588j$ |
| $[1-j,\ -1-j]^T$ | $0.4588-2.3066j$ |
| $[1-j,\ 1+j]^T$ | $1.5412+0.3066j$ |
| $[1-j,\ 1-j]^T$ | $2.3066-1.5412j$ |

As shown in Table 5.1, each $\boldsymbol{r}$ corresponds to a unique $\boldsymbol{\theta}^T\boldsymbol{r}$, vice versus.

After the matrix $\boldsymbol{\Gamma}$ is constructed and $\boldsymbol{\theta}$ is designed, the confidential information $\boldsymbol{s}$ is ready to be encoded by:

$$\boldsymbol{x} = \boldsymbol{\theta}^T\boldsymbol{\Gamma}, \tag{5.3}$$

where $\boldsymbol{x}$ is the transmitted symbol vector.

Here we consider a noiseless main channel and a BEC for eavesdropper with erasure rate $p_e$. Thus we have

$$\boldsymbol{y} = \boldsymbol{x} \ \ and \ \ \boldsymbol{z} = [z_1\ z_2 \cdots z_n] \tag{5.4}$$

such that $z_p = x_p$ with probability $p_l = 1 - p_e$ and $z_p$ is erased, i.e., $z_p$ =?, with probability $p_e$. $p_l$ is the leaked rate which describes the rate of information leaked to Eve.

In the following, we show that how Bob can perfectly recover $\boldsymbol{s}$ from $\boldsymbol{y}$. To be general, we assume Bob has complete knowledge of $\boldsymbol{\theta}$ but has no information about the random symbols that are chosen to construct $\boldsymbol{\Gamma}$. However, both Bob and Eve know that the random

symbols are chosen from QAM alphabet $\mathcal{S}$ with uniform distribution.

Based on the RCF code design with confidential symbols, random symbols and check symbols, we have

$$\sum_{q=1,\cdots,n} y_q = \sum_{q=1,\cdots,n} x_q = \boldsymbol{\theta}^T \boldsymbol{s} \tag{5.5}$$

where $x_q$ and $y_q$ represent, respectively, the $q$-th element of $\boldsymbol{x}$ and $\boldsymbol{y}$. The first equation in (5.5) holds from the noiseless main channel. while the second equation in (5.5) comes from (5.1). Thanks to the check symbols, the random symbols are canceled out. Hence, Bob can get the value of $\boldsymbol{\theta}^T \boldsymbol{s}$ by summing up all the symbols in $\boldsymbol{y}$. Since each symbol of $\boldsymbol{s}$ is a QAM symbol, Bob can easily find the exact confidential message $\boldsymbol{s}$ according to the one-to-one mapping between $\boldsymbol{\theta}^T \boldsymbol{s}$ and $\boldsymbol{s}$ [83].

**Result 1:** *Reliable transmission is achieved in noiseless main channel by RCF codes.*

## 5.3 Decoding strategy of Eve

In this section, we provide the optimal decoding strategy of Eve. Without loss of generality and reality, we have the following assumptions about Eve:

**EA1)** infinite computational power;

**EA2)** complete knowledge of $\boldsymbol{\theta}$;

**EA3)** knowledge of the general rule to construct $\boldsymbol{\Gamma}$;

**EA4)** no knowledge about the symbols that are chosen to construct $\boldsymbol{\Gamma}$;

**EA5)** if there are some check symbols $c_{p_1}$, $c_{p_2} \cdots c_{p_\mu}$ are in $\boldsymbol{\gamma}_q$ (the $q$-th column of $\boldsymbol{\Gamma}$), Eve can identify all the check symbols given $\boldsymbol{\theta}^T \cdot \boldsymbol{\gamma}_q$.

EA2), EA3) and EA4) are the same to the knowledge of the legitimate receiver Bob. Notice that $\boldsymbol{\gamma}_q$ may contain check symbols $c_p$ given by (5.1). By its definition, $c_p$ may or not belong to $\mathcal{S}$. For example, when 4-QAM symbols are employed, and $n = 3$, the check symbol $c_p = -((-1 - j + (1 + j))) = 0$, which is not in 4-QAM constellation. However,

the coordinates of $c_p$ are still some integers. Given the design of $\boldsymbol{\theta}$, Eve can still get the one-to-one mapping table between $\boldsymbol{\gamma}_q$ and $\boldsymbol{\theta}^T \cdot \boldsymbol{\gamma}_q$ and thus identify the check symbol $c_p$. But there are also probabilities that the check symbol $c_p$ is still in $\mathcal{S}$. For example, $c_p = -((1+j)+(-1-j)+(1+j)) = -1-j$, which is still in 4-QAM constellation. In such case, when $c_p$ is one of the symbols in $\boldsymbol{\gamma}_q$ and Eve has decoded all symbols in $\boldsymbol{\gamma}_q$, $c_p$ is mixed with other symbols in $\boldsymbol{\gamma}_q$, and thus Eve can not determine the check symbol. In the following discussion, though it is not the true case, we assume Eve always has the ability to determine the check symbol from other symbols when it is in $\boldsymbol{\gamma}_q$. Based on these assumptions about Eve, we first discuss the optimal decoding strategy of Eve. Next, the secure performance about RCFC based on the optimal decoding strategy is analyzed.

Notice that when the elements in each row of $\boldsymbol{\Gamma}$ have been generated, by permutating the symbols in the same row, we can have different $\boldsymbol{\Gamma}$ which still satisfy the construction rules of $\boldsymbol{\Gamma}$. Hence the number of possible $\boldsymbol{\Gamma}$ with these elements is $(P_n^n)^m$, where $P_n^k$ is the $k$-th falling factorial power of $n$. Since all the permutations in each row of $\boldsymbol{\Gamma}$ are considered in the following discussions, we assume the first $\lfloor n \times p_l \rceil$ symbols are leaked to Eve, which means

$$\boldsymbol{z} = [z_1\ z_2 \cdots z_n] = [x_1\ x_2 \cdots x_{np_l}\ ? \cdots ?]. \tag{5.6}$$

Via (5.3), we have

$$z_q = \begin{cases} \boldsymbol{\theta}^T \boldsymbol{\gamma}_q & \text{if } q = 1, \cdots, \lfloor np_l \rceil \\ ? & \text{if } q = \lfloor np_l \rceil + 1, \cdots, n \end{cases} \tag{5.7}$$

where $\boldsymbol{\gamma}_q = [\gamma_{1,q}\ \gamma_{2,q}, \cdots, \gamma_{n,q}]^T$. By the above assumption about Eve, all symbols in $\boldsymbol{\gamma}_1,\ \boldsymbol{\gamma}_2, \cdots, \boldsymbol{\gamma}_{np_l}$ can be decoded by Eve.

Now we focus on how Eve should decode $s_1$ based on the decoded symbols in the set $\{\boldsymbol{\gamma}_1,\ \boldsymbol{\gamma}_2, \cdots, \boldsymbol{\gamma}_{np_l}\}$. Since the symbols in different rows are independent to each other, only the decoded symbols in the first row of $\boldsymbol{\Gamma}$ may leak information about $s_1$ to Eve. Denote the set of the decoded symbols of the first row of $\boldsymbol{\Gamma}$ as $\mathcal{D}_1$. According to our assumptions, we have $\mathcal{D}_1 = \{\gamma_{1,1}\ \gamma_{1,2}, \cdots \gamma_{1,np_l}\}$. Via the construction rules of $\boldsymbol{\Gamma}$, there are four possible

combinations of $\mathcal{D}_1$ which are listed as follows:

1. $\{\gamma_{1,1}\ \gamma_{1,2}, \cdots \gamma_{1,np_l}\}$ is only composed of random symbols $\{u_{1,1}\ u_{1,2}, \cdots u_{1,np_l}\}$.
2. $\{\gamma_{1,1}\ \gamma_{1,2}, \cdots \gamma_{1,np_l}\}$ is composed of confidential symbol $s_1$ and random symbols.
3. $\{\gamma_{1,1}\ \gamma_{1,2}, \cdots \gamma_{1,np_l}\}$ is composed of check symbol $c_1$ and random symbols.
4. $\{\gamma_{1,1}\ \gamma_{1,2}, \cdots \gamma_{1,np_l}\}$ is composed of confidential symbol $s_1$, check symbol $c_1$ and random symbols.

In the first two combinations, since the check symbol $c_1$ is not decoded, Eve can not know whether $s_1$ is in $\mathcal{D}_1$ or not. For such combinations, the optimal decoding strategy for Eve is randomly choosing one symbol $\gamma_{1,q}$ from $\mathcal{D}_1$ as $s_1$. When Eve adopts this decoding strategy and the symbols in $\mathcal{D}_1$ are the first combination, the probability that $s_1$ can be decoded is $P(s_1 = \gamma_{1,q}) = \frac{1}{M}$. When it is the second combination, *i.e.*, $s_1 \in \mathcal{D}_1$, we have

$$\begin{aligned} P(s_1 = \gamma_{1,q}) &= P(s_1 = u_{1,*}|\gamma_{1,q} = u_{1,*})P(\gamma_{1,q} = u_{1,*}) \\ &\quad + P(s_1 = s_1|\gamma_{1,q} = s_1)P(\gamma_{1,q} = s_1) \\ &= \frac{np_l - 1}{np_l} \cdot \frac{1}{M} + \frac{1}{np_l} \approx \frac{1}{M} \end{aligned} \tag{5.8}$$

where $u_{1,*}$ is any random symbol in the first row of $\mathbf{\Gamma}$. The last approximation in (5.8) approaches $P(s_1 = \gamma_{1,q})$ closely with large code length $n$ and fixed leaked rate $p_l$.

For EA3) and EA4), $c_1$ is known by Eve. The optimal decoding strategy for Eve is given by two different cases:

*Case 1:* Check if there exist $np_e - 1$ symbols $u_{e_1}, , u_{e_2}, \cdots u_{e_{np_e}}$ from $\mathcal{S}$ such that

$$c_1 + \Big( \sum_{q=1,\cdots,np_l} \gamma_{1,q} - c_1 \Big) = - \sum_{l=1,\cdots,np_e-1} u_{e_l} \tag{5.9}$$

If (5.9) holds, it means $-c_1$ is the summation of the symbols in $\mathcal{D}_1 \setminus c_1$ and some other random symbols $u_{e_1}, , u_{e_2}, \cdots u_{e_{np_e}}$. The $np_e - 1$ random symbols in (5.9) are taken by Eve as part of those erased symbols. Given by the definition of $c_1$, it is the summation of all the

random symbols. Therefore, $s_1$ is successfully mixed with other random symbols no matter whether $s_1$ is in $\mathcal{D}_1$ or not. Under such case, Eve can only randomly choose one symbol from $\mathcal{D}_1 \setminus c_1$ as $s_1$.

*Case 2:* If there are not such symbols that satisfy (5.9), then Eve knows that $s_1$ must be in $\mathcal{D}_1$. Eve can judge whether $\gamma_{1,k}$ in $\mathcal{D}_1 \setminus c_1$ is suspicious or not by checking whether $\gamma_{1,k}$ satisfies the following inequations:

$$c_1 + \Big( \sum_{q=1,\cdots,np_l} \gamma_{1,q} - c_1 - \gamma_{1,k} \Big) \neq - \sum_{l=1,\cdots,np_e} u_{e_l}, \ \forall u_{e_l} \in \mathcal{S}, \tag{5.10}$$

where $k = 1, \ 2 \cdots, np_l$ and $\gamma_{1,k} \neq c_1$. If the inequality (5.10) holds, then $\gamma_{1,k}$ is suspected as $s_1$ by Eve. Sequentially checking each symbol in $\mathcal{D}_1 \setminus c_1$, Eve can find out all suspicious symbols. Denote the set of all the suspicious symbols as $\mathcal{D}_{s_1}$. $s_1$ is decoded by randomly choosing one symbol from $\mathcal{D}_{s_1}$.

In summary, the optimal decoding strategy for Eve is presented as follows:

*Step 1:* Based on the observation $\boldsymbol{z}$ and the one-to-one mapping between $\boldsymbol{\theta}^T \cdot \boldsymbol{\gamma}_q$ and $\boldsymbol{\gamma}_q$, Eve first decodes $\boldsymbol{\gamma}_1, \ \boldsymbol{\gamma}_2 \cdots, \ \boldsymbol{\gamma}_{np_l}$. The set of the decoded symbols in the first row of $\mathbf{\Gamma}$ is $\{\gamma_{1,1} \ \gamma_{1,2}, \cdots \gamma_{1,np_l}\}$, which is denoted as $\mathcal{D}_1$.

*Step 2:* Judge whether $c_1$ is in $\mathcal{D}_1$ or not. If not, Eve just decodes $s_1$ by randomly choosing one symbol from $\mathcal{D}_1$. If $c_1 \in \mathcal{D}_1$, Eve follows the methods in *Case 1* and *Case 2* to decode $s_1$.

*Step 3:* Decode $s_2, \ s_3 \cdots, s_m$ by repeating *Step 2* with the corresponding $\mathcal{D}_p$, for $p = 2, \ 3 \cdots, m$.

## 5.4 Security Analysis of RCF Codes

We have presented the decoding strategy of both Bob and Eve. Now let us analyze the security performance of RCFC based on the proposed decoding strategy. In this section, unless specified, all the results are based on noiseless main channel and BEC for wiretapper. The security performance of RCFC is analyzed from two aspects, *i.e.,* the probability that Eve can correctly decode $\boldsymbol{s}$ and the mutual information between $\boldsymbol{s}$ and $\boldsymbol{z}$.

### 5.4.1 Decoding Ability of Eve

We have shown that if $c_1 \notin \mathcal{D}_1$, the probability that $s_1$ is successfully decoded is $\frac{1}{M}$. Now we discuss the correct decoding probability when $c_1 \in \mathcal{D}_1$.

If $\mathcal{D}_1$ is composed of $c_1$ and random symbols, Eve will decode $s_1$ via the methods in *Case 1* and *Case 2*. Since $s_1 \notin \mathcal{D}_1$, thus (5.9) must hold. Eve can only randomly choose one symbol $\gamma_{1,p}$ from $\mathcal{D}_1 \setminus c_1$ as $s_1$. Under such situation, the probability that $s_1$ can be successfully decoded by Eve is $P(s_1 = \gamma_{1,q}) = \frac{1}{M}$. If both $s_1$, $c_1$ are in $\mathcal{D}_1$, Eve will choose one symbol from the suspicious set $\mathcal{D}_{s_1}$ generated from the results of *Case 2*. In that case, the probability that $s_1$ can be successfully decoded is $1/E\left[|\mathcal{D}_{s_1}|\right]$, where $E[\cdot]$ is the expectation and $|\mathcal{D}_{s_1}|$ is the size of $\mathcal{D}_{s_1}$, *i.e.,* the number of different symbols in $\mathcal{D}_{s_1}$. Moreover, for any other suspicious set of $s_p$, we have

$$E\left[|\mathcal{D}_{s_p}|\right] = E\left[|\mathcal{D}_{s_1}|\right]. \tag{5.11}$$

Summarizing all probabilities that $s_1$ can be successfully decoded and (5.11), the following lemma can be proved.

**Lemma 5.4.1** *For noiseless main channel and BEC for wiretapper, when RCFCs are employed, the probability that $s_p, \forall p = 1, 2 \cdots, m$ can be successfully decoded is given by:*

$$P\left(\hat{s}_p = s_p\right) = \begin{cases} 1/E\left[|\mathcal{D}_{s_1}|\right], & \text{if } c_p \in \mathcal{D}_p \text{ and } s_p \in \mathcal{D}_p; \\ \frac{1}{M}, & \text{otherwise.} \end{cases} \tag{5.12}$$

*where $\hat{s}_p$ is the estimation of $s_p$ given by Eve.*

Notice that $E\left[|\mathcal{D}_{s_1}|\right]$ in (5.12) depends on constellation size, the length of confidential information $m$, codeword length $n$ and the erasure rate $p_e$ of the BEC. It is difficult (if not impossible) to get the analytical expression of $E\left[|\mathcal{D}_{s_1}|\right]$. Here, the following lemma gives a lower bound of $E\left[|\mathcal{D}_{s_1}|\right]$.

**Lemma 5.4.2** *When $c_p \in \mathcal{D}_p$ and $s_p \in \mathcal{D}_p$, given the QAM constellation size $M$, the erasure rate of the wiretapper's channel $p_e$ and the codeword length $n$, we have*

$$E\left[|\mathcal{D}_{s_p}|\right] \geq \left[1 - \left(1 - \frac{1}{M}\right)^{np_e}\right] \cdot M. \tag{5.13}$$

Now we are ready to present the upper bound of the probability that Eve can successfully decode $\boldsymbol{s}$.

**Theorem 5.4.3** *Given the erasure rate of BEC $p_e$, the probability that Eve can successfully decode the confidential message $\boldsymbol{s}$ via his observation $\boldsymbol{z}$ is upper bounded by*

$$P(\hat{\boldsymbol{s}} = \boldsymbol{s}|\boldsymbol{z}) \leq \left[\frac{(P_{n-2}^{n-2}P_{p_In}^2)^{\frac{1}{A}} + (P_n^n - P_{n-2}^{n-2}P_{p_In}^2)^{\frac{1}{M}}}{P_n^n}\right]^m \tag{5.14}$$

*where $P_n^k$ is the k-th falling factorial power of $n$, $\hat{\mathbf{s}}$ is the estimated confidential information given by Eve via $\boldsymbol{z}$ and*

$$A = \left[1 - (1 - \frac{1}{M})^{np_e}\right] \cdot M. \tag{5.15}$$

Now, two critical questions here are:

1. Whether $P(\hat{\boldsymbol{s}} = \boldsymbol{s}|\boldsymbol{z})$ converges with fixed erasure rate and secrecy rate when $n \to \infty$?
2. If yes, what does it converge to?

To answer these two questions, we need the following lemma.

**Lemma 5.4.4** *Given the erasure rate of BEC $p_e$ and the secrecy rate $m/n$, if the secrecy rate $m/n$ is below or equal to the secrecy capacity (which is $p_e$ for the channel model considered in this paper), then we have*

$$\left[1 - (1 - \frac{1}{M})^{np_e}\right]^i \to 1 \text{ as } n \to \infty, \tag{5.16}$$

*where $i = 1, \cdots, m$.*

Now we are ready to answer the above two questions by the following Corollary.

**Corollary 5.4.5** *Given the erasure rate of the wiretap channel $p_e$ and the secrecy rate $m/n$, when the secrecy rate is less than or equal to the secrecy capacity, i.e., $m/n \leq p_e$, the probability that Eve can successfully decode $\boldsymbol{s}$ converges to the probability that Eve randomly chooses m symbols from $\mathcal{S}$ which are exactly the symbols of $\boldsymbol{s}$, i.e., $P(\hat{\boldsymbol{s}} = \boldsymbol{s}|\boldsymbol{z}) \rightarrow \left(\frac{1}{M}\right)^m$ as $n \rightarrow \infty$.*

The proof is straightforward from Lemma 5.4.4.

So far, we derive an easily computed upper bound of the probability that Eve can successfully decode $\boldsymbol{s}$ from $\boldsymbol{z}$. We have also shown that with fixed $p_e$ and the secrecy rate $m/n$, if we increase the codeword length $n$, Eve's decoding ability is reduced. More extremely, when the secrecy rate is less than or equal to the secrecy capacity of the wiretap channel, as $n \rightarrow \infty$, RCF codes totally hide the confidential information $\boldsymbol{s}$ among all possible symbols from the same QAM constellation $\mathcal{S}$ for Eve, i.e., the observation of Eve $\boldsymbol{z}$ can not provide any information about $\boldsymbol{s}$ for Eve.

### 5.4.2 Achievable Security Information Rate of RCFC

In this section, we investigate the security performance of RCF codes. Different from binary coding scheme, RCF codes are non-binary codes. Hence we define the *normalized security information rate* as follows (which is later shown to be a metric of how secure a transmission is):

**Definition 1:** the *normalized security information rate* $R_{NS}$ is defined as

$$R_{NS} = \frac{\mathcal{I}(\boldsymbol{s};\boldsymbol{y}) - \mathcal{I}(\boldsymbol{s};\boldsymbol{z})}{\mathcal{H}(\boldsymbol{s})}, \tag{5.17}$$

where $\mathcal{I}(\boldsymbol{s};\boldsymbol{y})$ represents the mutual information between $\boldsymbol{s}$ and $\boldsymbol{y}$ and $\mathcal{H}(\cdot)$ is the entropy.

By the definition of the *normalized security information rate*, we have the following property about it:

**Lemma 5.4.6** *Given noiseless main channel and BEC of wiretapper,* $0 \leq R_{NS} \leq 1$.

By definition, $R_{NS} = 1$ is equivalent to $\mathcal{H}(\boldsymbol{s}|\boldsymbol{z}) = \mathcal{H}(\boldsymbol{s})$, which means

$$\mathcal{I}(\boldsymbol{s};\boldsymbol{z}) = \mathcal{H}(\boldsymbol{s}) - \mathcal{H}(\boldsymbol{s}|\boldsymbol{z}) = 0, \tag{5.18}$$

i.e., $\boldsymbol{z}$ can not provide any information about $\boldsymbol{s}$. If $R_{NS} = 0$, then given $\boldsymbol{z}$, $\boldsymbol{s}$ can be decoded. Hence $R_{NS}$ is a metric to measure how secure the transmission is. The larger $R_{NS}$ is, the more secure $\boldsymbol{s}$ is. Therefore, in the following, we focus on analyzing $R_{NS}$ for RCFC over the wiretap channel.

For noiseless main channel and binary erasure wiretapper's channel, the following theorem gives a lower bound of $R_{NS}$ that can be achieved by RCF codes.

**Theorem 5.4.7** *Given the secrete rate $m/n$ and leak rate of BEC $p_l$, the normalized security information rate that can be achieved by RCF codes is lower bounded by:*

$$R_{NS} \geq \frac{1}{m\log_2 M}\sum_{k=0}^{m}\binom{m}{k}\frac{(P_{n-2}^{n-2}P_{p_l n}^2)^{m-k}(P_n^n - P_{n-2}^{n-2}P_{p_l n}^2)^k}{(P_n^n)^m} \cdot \log_2(M^k \cdot A^{m-k}), \tag{5.19}$$

*where $\binom{m}{k}$ is the number of k combination of an m-set without repetition.*

Theorem 5.4.7 reveals the fundamental relationship between the lower bound of $R_{NS}$ achieved by RCF codes and the parameters of the channel and the codes. According to the results given in Theorem 5.4.7, it is easy to estimate the performance the RCF codes given $p_e$, code rate $\frac{m}{n}$ and the QAM constellation $\mathcal{S}$. But the true transmission should be more secure than the estimation given in Theorem 5.4.7. On the other side, given the desired $R'_{NS}$ and $p_e$, Theorem 5.4.7 offers a way to design the RCF codes which is described as follows:

1. Initilize $m$, $n$ and $\boldsymbol{S}$;
2. Compute the lower bound of $R_{NS}$ given in Theorem 5.4.7 with chosen $m$, $n$ and $\boldsymbol{S}$;
3. If the lower bound of $R_{NS}$ is larger than or equal to $R'_{NS}$, then the chosen $m$, $n$ and $\boldsymbol{S}$ should satisfy the requirement; If not, adjust some or all of the parameters and start over from step 2.

Next, we show that RCF codes can achieve the secrecy capacity asymptotically.

**Corollary 5.4.8** *Given the erasure rate of the wiretapper's binary erasure channel $p_e$ and the secrecy rate $\frac{m}{n}$ of RCF codes, when $m/n \leq p_e$, $R_{NS} \to 1$ as $n \to \infty$, i.e., the RCF codes can achieve the secrecy capacity as the codeword length n goes to infinity.*

In this section, we have shown that when the secrecy rate is less than or equal to the channel erasure rate, Eve can only blindly choose the information symbols as $n \to \infty$. In other words, RCF codes can achieve the secrecy capacity.

## 5.5 The Analysis of the Computation Complexity

In this section, we compare the computation complexity for Bob and Eve. From the decoding strategies of Bob and Eve, both of them need to construct a look-up table between a $m \times 1$ column vector $\boldsymbol{r}$ and the value of $\boldsymbol{\theta}^T \cdot \boldsymbol{r}$. We focus on the size of the two different look-up tables that Bob and Eve needs to construct. Actually, even with existing look-up tables, the strategies for Bob and Eve have shown that the operations in Eve's decoding are far more complex than Bob's. However, those operations in the decoding steps are not the concern here.

Let us first consider the look-up table for Bob. As shown in (5.5), after summing all the symbols in Bob's observation $\boldsymbol{y}$, he gets the value $\boldsymbol{\theta}^T \cdot \boldsymbol{s}$. Hence Bob only need to construct a look-up table showing the relationship between $\boldsymbol{s}$ and $\boldsymbol{\theta}^T \cdot \boldsymbol{s}$. When the size of QAM constellation is $M$ and there are $m$ confidential symbols in $\boldsymbol{s}$, the number of the possible values of $\boldsymbol{\theta}^T \cdot \boldsymbol{s}$ is $M^m$, thus the size of the table for Bob is $M^m$.

Different from Bob, Eve can only get $\{\boldsymbol{\theta}^T \cdot \boldsymbol{\gamma}_1, \ \cdots, \boldsymbol{\theta}^T \cdot \boldsymbol{\gamma}_{np_l}\}$. The possible symbols in $\boldsymbol{\gamma}_q$ include the information symbols, the random symbols and the check symbols. By the definition of the check symbol given in (5.1), there are $M^{n-2}$ possible check symbols (Since there may be some repetitions, the actual number of possible check symbols should be less than $M^{n-2}$. However, since the decoding strategy of Eve requires to find out all the possible combinations of random symbols that generate the same check symbol, we take

those check symbols with the same value as different ones). Hence the size of the look-up table of Eve is at least $\left(M^{n-2} \times M\right)^m$.

Table 5.2 shows the size of the look-up tables for Eve and Bob and the ratio between them. From Table 5.2 we can see that the difference in the size is quite impressive. It is also shown in this table that the length of the codeword will not change the size of the look-up table for Bob but it hugely increases the one for Eve. Furthermore, if we increase $m$ and $n$ simultaneously to keep the code rate $\frac{m}{n}$ unchanged, the size for Bob is increased by $M^m$, but the size for Eve is increased by $M^{m\times(n-1)}$. Therefore, increasing the length of the codeword is an effective way to increase the decoding complexity for Eve.

**Table 5.2. The size of the look-up tables for Bob and Eve**

| The parameters | Bob | Eve | Eve/Bob |
|---|---|---|---|
| $M = 4,\ m = 5,\ n = 10$ | 1024 | $> 4^{45}$ | $> 4^{40}$ |
| $M = 8,\ m = 10,\ n = 20$ | $8^{10}$ | $> 8^{190}$ | $> 8^{180}$ |
| $M = 16,\ m = 10,\ n = 20$ | $16^{10}$ | $> 16^{190}$ | $> 16^{180}$ |
| $M = 8,\ m = 10,\ n = 30$ | $8^{10}$ | $> 8^{290}$ | $> 8^{280}$ |
| $M = 8,\ m = 15,\ n = 30$ | $8^{15}$ | $> 8^{435}$ | $> 8^{420}$ |

## 5.6 Numerical Results

The performance of the proposed RCF codes is evaluated by estimating the upper bound of the probability that Eve can successfully decode the confidential information $\boldsymbol{s}$ and the lower bound of the normalized security information rate achieved by RCF codes. The numerical results are presented by different example studies.

**Example 3:** Given $M = 16$ *and* $m = 10$, Fig.5.4 depicts the upper bounds of the probabilities given in (5.14) that Eve can successfully decode the confidential information $\boldsymbol{s}$ via his observation $\boldsymbol{z}$ with different codeword length $n$.

We observe that with the same erasure rate $p_e$, the larger $n$ is, the smaller the upper

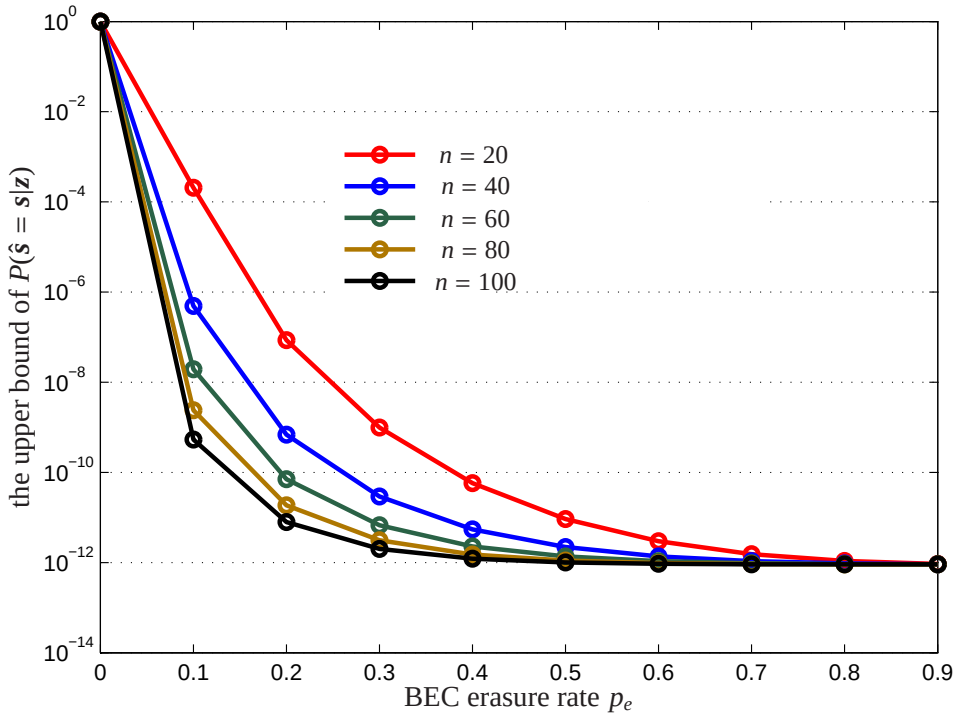



**Figure 5.4. The upper bound of $P(\hat{s} = s|z)$ from Theorem 5.4.3 for QAM constellation with different code length $n$.** $M = 16,\ m = 10$.

bound of $P(\hat{\boldsymbol{s}} = \boldsymbol{s}|\boldsymbol{z})$ is. Hence increasing $n$ reduces the probability that $\boldsymbol{s}$ can be successfully decoded by Eve. But as shown in Fig. 5.4, when $m/n > p_e$, the upper bound of $P(\hat{\boldsymbol{s}} = \boldsymbol{s}|\boldsymbol{z})$ can not approach $(\frac{1}{M})^m$ (In this example,$\log_{10}(\frac{1}{M})^m \approx -12$). However when $m/n \leq p_e$, $P(\hat{\boldsymbol{s}} = \boldsymbol{s}|\boldsymbol{z})$ approaches $(\frac{1}{M})^m$, asymptotically. The curves match well with the result in Corollary 1. Actually, $P(\hat{\boldsymbol{s}} = \boldsymbol{s}|\boldsymbol{z}) = (\frac{1}{M})^m$ means Eve can not get any information about $\boldsymbol{s}$ from his observation and can just randomly pick $m$ symbols from $\mathcal{S}$ as $\boldsymbol{s}$. Fig. 5.4 shows that the proposed RCF codes can decrease the decoding probability of Eve by increasing the codeword length $n$. When the secrecy rate $m/n$ is below or equal to the secrecy capacity of the wiretap channel, which is $p_e$ in this example, the decoding probability of Eve approaches $(\frac{1}{M})^m$ as $n$ goes to infinity.

**Example 4:** Given $n = 100$ *and* $m = 10$, Fig.5.5 plots the upper bounds of the probabilities that Eve can successfully decode the information $\boldsymbol{s}$ with different sizes of the QAM constellations $M$.

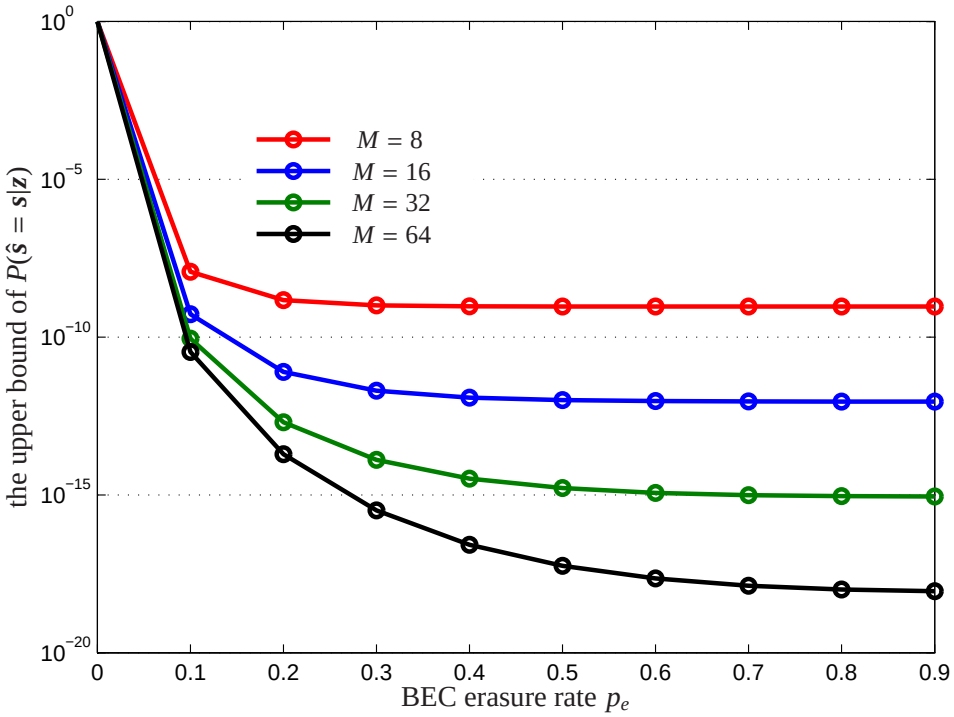



**Figure 5.5. The upper bound of $P(\hat{s} = s|z)$ from Theorem 5.4.3 for QAM constellation with different QAM constellation size $M$. $n = 100,\ m = 10$.**

In this case, the larger $M$ is, the smaller the upper bound of $P(\hat{\boldsymbol{s}} = \boldsymbol{s}|\boldsymbol{z})$ is, which means increasing the size of the constellation can reduce the probability that $\boldsymbol{s}$ can be successfully decoded by Eve. But, increasing $M$ will also increase decoding complexity for both Bob and Eve. Hence it may not be the practical method to realize the secure transmission.

**Example 5:** Given $m = 10$, Fig.5.6 plots the lower bounds of the normalized security information rate $R_{NS}$ achieved by RCF codes with different length of the codeword $n$ and different constellation sizes $M$.

The results in Fig.5.6 are from Theorem 5.4.7. With fixed $p_e$, the larger $n$ induces that $R_{NS}$ approaches 1 faster. Hence, increasing the length of RCF codes can improve the security of the transmission over wiretapper's channel. In Example 3, we have shown that larger $M$ brings smaller upper bound of the probability that $\boldsymbol{s}$ can be successfully decoded by Eve. But the situation is different for $R_{NS}$. As shown in Fig.5.6, with the same $p_e$, the larger $M$ is, the smaller the lower bound of $R_{NS}$ is. Therefore, given $p_e$ and the code rate of RCF codes, to simultaneously achieve low decoding ability of Eve and high $R_{NS}$ of the

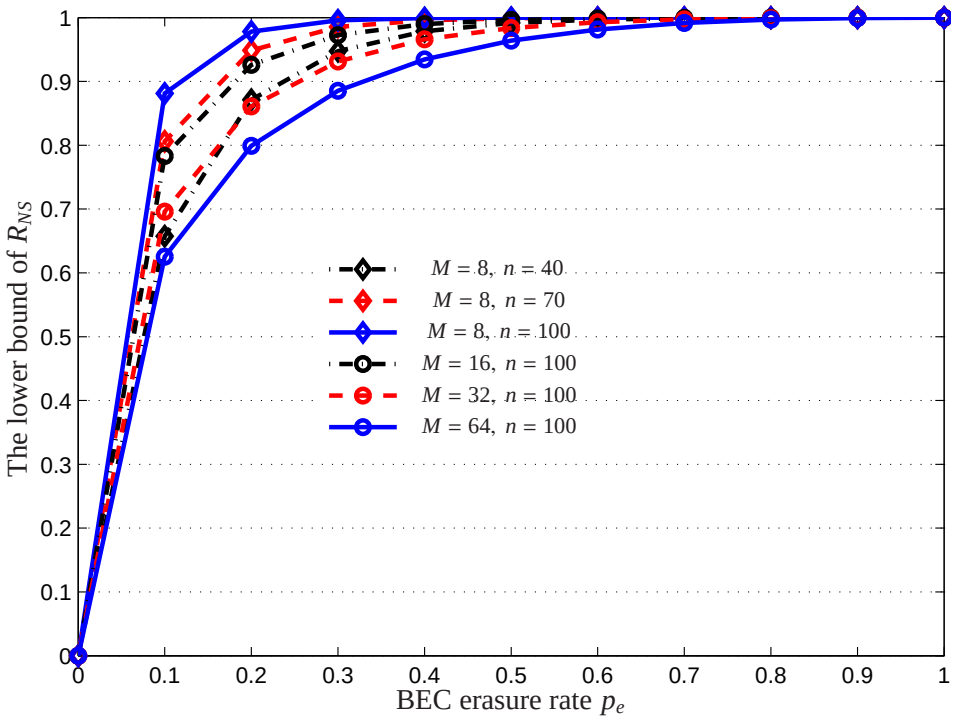



**Figure 5.6. The lower bound of $R_{NS}$ from Theorem 5.4.7 with different length of the codeword $n$ and different constellation size $M$.**

channel, increasing the length of RCF codes is the effective way.

These numerical results have verified both Theorems 5.4.3 and 5.4.7. Also they illustrate the flexibility of our design with different secrecy rate. With the constraint of $m/n \leq p_e$, as the codeword length goes to infinity, the normalized security information rate reaches the optimal value 1.

## 5.7 Conclusion and Future Directions

In this chapter, we present RCFC to achieve the security over wiretap channel with noiseless main channel and binary erasure wiretap's channel. It has been shown that RCF codes are easy and flexible to design with any given secrecy rates. We also prove that RCF codes can achieve the secrecy capacity asymptotically with the codeword length goes to infinity. Moreover, when the secrecy rate is below the secrecy capacity, secure communication can be realized by RCFC. Furthermore, the proposed design is the first one which provides a

platform to tradeoff secrecy performance with the erasure rate of the eavesdropper's channel and the secrecy rate.

However, the performance of RCFCs for noisy channel is still an open problem. When RCFCs are applied for wireless communications, more work needs to be studied for fading main and wiretapper's channels.

# CHAPTER 6

# CONCLUSION

In this dissertation, we have studied signal detection and security code design from information theoretic point of view. The main contributions are summarized as follows.

we have developed a computationally efficient sub-optimal detection algorithm and coding scheme for 2-D ISI channel with M-ary inputs by using multilevel coding and multistage decoding. The fundamental idea is to equalize the channel stage by stage. To begin with the stage with the highest signal power level, the multi-strip BCJR algorithm is used to equalize each level by averaging the interference of the undecoded levels. Both the hard and soft decisions are passed to the next stages. To reduce the computation complexity, instead of using full-branch BCJR on the entire received page of data, the BCJR algorithm is only employed on reduced states by considering the bits from the undetected levels as independently and identically distributed with equal probability. Furthermore, the distribution of the output given the data of the detected levels is approximated by a Gaussian distribution. Both the mean and the variance of the approximated distribution can be computed offline. Using the approximation, the data on the current stage can be decoded without considering the data from undetected levels. Hence the number of states at each stage is kept at $2^{L_x \times L_y}$. With the proposed detection scheme, we also compute the achievable information rate on each level. More over, the corresponding component LDPC code is designed accordingly to achieve the achievable information rate with the proposed detection algorithm. Both numerical and simulation results have demonstrated the significant performance of the proposed detection algorithm in detecting signals through M-ary 2D ISI channels.

For the discrete MIMO channel with MLD or ZFD, we first established a new metric, the post-detection mutual information (PMI), to quantify the ultimate information rate between the discrete inputs and the hard detected output. This is the first time that the information rate loss caused by the hard mapping of the detectors is considered. Since the hard

mapping step in the detector is irreversible, we expect that the PMI is reduced compared to the MI without hard mapping. The conclusion is confirmed by both the simulation and the theoretic results. Consequently, the ultimate achievable PMI rates that can be transmitted through the MIMO channels with MLD or ZFD serve as more practical benchmarks for transmissions. Next, we derive the analytical expression of the PMI with MLD or ZFD. We have shown that there is no closed form formula of for the PMI. However, the easily computed asymptotically lower bounds of them are proposed for PSK constellations. The lower bounds also serve as the approximations. Moreover, when QAM constellations are adopted, we provide the numerical form for the PMI with ZFD. The values obtained from the numerical formula match exactly the results from the simulations. We have also shown that when $od(\boldsymbol{H}) = 0$, the PMI with MLD or ZFD is equal to each other which is consistent with the case for the MI with ML and ZF receiver. All of the research results about the PMI have been verified by the simulation results.

To achieve the secure transmission over wiretap channel with noiseless main channel and BEC wiretapper's channel, we have proposed a non-binary security code design by using random complex field coding (RCFC) technique. The key idea for RCFC is to mix some random symbols with the information symbols so that Eve cannot decode information symbols but Bob still can. The RCF codes are easy to design with any given code rates. We have shown that when the erasure rate of BEC is greater than zero, RCFC can achieve the secrecy capacity asymptotically. Moreover, when the secrecy rates are below the secrecy capacity, RCFC can realize perfectly secrete communication, *i.e.*, both reliability and security can be achieved simultaneously. We have also demonstrated that the decoding for Bob is extremely easy, which is just checking a look-up table. However, Eves' computation complexity is rapidly and hugely increased with the codeword length. Even though Eve did a very complex computation, as long as the secrecy rates are below the secrecy capacity, we can design a RCFC such that the decoding of Eve is just blindly guessing the information symbols from the transmission constellation. More importantly, in addition to approaching

the secrecy capacity, the proposed code design is the first one which provides a platform to tradeoff secrecy performance with the erasure rate of the eavesdropper's channel and the secrecy rate. Hence, the RCFC can be designed as required by the users or the providers. While, there are no such tradeoffs available for LDPC codes. The significant performance of RCFC has been confirmed by both the numerical and simulation results.

# APPENDIX A

# PROOF FOR CHAPTER 3

## A.1 Proof of Proposition 3.3.1

In this appendix, we show how to derive Proposition 3.3.1. According to central limited theorem, $P\left(y(i,j)|\hat{d}^{(k+1:K)}(i-L_y:i,j-L_x,j),d^{(k)}(i-L_y:i,j-L_x,j)\right)$ can be approximated by a Normal distribution. The mean of the approximated Normal distribution is the expectation value of $y(i,j)$ given $\hat{d}^{(k+1:k)}(i-L_y:i,j-L_x:j)$, $d^{(k)}(i-L_y:i,j-L_x:j)$, and $\tilde{d}^{(1:k-1)}(i-L_y:i,j-L_x:j)$, thus we have

$$\begin{aligned}
&\hat{\mu}_{(k)}\left(\tilde{d}^{(1:k-1)}(i,j)\right)\\
&=E\left[y(i,j)|\hat{d}^{(k+1:k)}(i-L_y:i,j-L_x:j),d^{(k)}(i-L_y:i,j-L_x:j),\tilde{d}^{(1:k-1)}(i-L_y:i,j-L_x:j)\right]\\
&=h(0,0)x(i,j)+\sum_{p=1}^{L_x}\sum_{q=1}^{L_y}h(p,q)x^{(k:K)}(i-p,j-q)\\
&\qquad\qquad+\frac{1}{W}\sum_{p=1}^{L_x}\sum_{q=1}^{L_y}\sum_{\tilde{d}^{(1:k-1)}(i-p,j-q)}h(p,q)x^{(1:k-1)}(i-p,j-q).
\end{aligned}\tag{A.1}$$

In (A.1), the first term on the right-hand side can be calculated by

$$h(0,0)x(i,j)=h(0,0)\left[\sum_{k'=k+1}^{K}\sqrt{P^{k'}}\hat{d}^{(k')}(i,j)+\sqrt{P^{k}}d^{(k)}(i,j)+\sum_{k'=1}^{k-1}\sqrt{P^{k'}}\tilde{d}^{(k')}(i,j)\right]=A_0.\tag{A.2}$$

The second term on the right-hand side is

$$\begin{aligned}
&\sum_{p=1}^{L_x}\sum_{q=1}^{L_y}h(p,q)x^{(k:K)}(i-p,j-q)\\
&=\sum_{p=1}^{L_x}\sum_{q=1}^{L_y}h(p,q)\left[\sum_{k'=k+1}^{K}\sqrt{P^{k'}},\hat{d}^{(k')}(i,j)+\sqrt{P^{k}}d^{(k)}(i,j)\right]\\
&=A_1.
\end{aligned}\tag{A.3}$$

and

$$\begin{aligned}
&\sum_{p=1}^{L_x}\sum_{q=1}^{L_y} h(p,q)x^{(1:k-1)}(i-p,j-q) \\
&= \sum_{p=1}^{L_x}\sum_{q=1}^{L_y} h(p,q)\left[\sum_{k'=1}^{k-1}\sqrt{P^{k'}}\tilde{d}^{(k')}(i-p,j-q)\right] \\
&= A_2. \qquad \text{(A.4)}
\end{aligned}$$

Plug (A.2), (A.3), and (A.4) in (A.1), (3.17) can be derived.

The variance of the approximated distribution $\hat{\sigma}^2_{(k)}\left(\tilde{d}^{(1:k-1)}(i,j)\right)$ can be derived from

$$\begin{aligned}
\hat{\sigma}^2_{(k)}\left(\tilde{d}^{(1:k-1)}(i,j)\right) &= E\left\{\left|y(i,j)-\hat{\mu}_{(k)}\left(\tilde{d}^{(1:k-1)}(i,j)\right)\right|^2 \,\middle|\, \begin{array}{l} \hat{d}^{(k+1:k)}(i-L_y:i, j-L_x:j), \\ d^{(k)}(i-L_y:i, j-L_x:j), \\ \tilde{d}^{(1:k-1)}(i-L_y:i, j-L_x:j) \end{array}\right\} \\
&= \frac{1}{W}\sum_{\tilde{d}^{(1:k-1)}(i-L_x:i,\, j-L_y:j)} \left|A_0+A_1+A_2-\hat{\mu}_{(k)}\left(\tilde{d}^{(1:k-1)}(i,j)\right)\right|^2. \qquad \text{(A.5)}
\end{aligned}$$

# APPENDIX B

# PROOF FOR CHAPTER 4

## B.1 Proof of Proposition 4.2.1

From the definition of PMI with MLD given in Definition 4.1.1, we have

$$
\begin{aligned}
&\mathcal{I}(\boldsymbol{s};\hat{\boldsymbol{s}}_{ML}|\boldsymbol{H}) \\
&\quad= \mathcal{H}(\boldsymbol{s}) - \mathcal{H}(\boldsymbol{s}|\hat{\boldsymbol{s}}_{ML},\boldsymbol{H}) \\
&\quad= M\log_2 q + \sum_{\boldsymbol{s}_v\in\mathcal{S}^M} P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{H})\left(\sum_{\boldsymbol{s}_u\in\mathcal{S}^M} P(\boldsymbol{s}=\boldsymbol{s}_u|\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v,\boldsymbol{H})\log_2 P(\boldsymbol{s}=\boldsymbol{s}_u|\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v,\boldsymbol{H})\right) \\
&\quad= M\log_2 q + \sum_{\boldsymbol{s}_v\in\mathcal{S}^M}\left(\sum_{\boldsymbol{s}_p\in\mathcal{S}^M} P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\tilde{\boldsymbol{s}}=\boldsymbol{s}_p,\boldsymbol{H})P(\tilde{\boldsymbol{s}}=\boldsymbol{s}_p)\right) \\
&\qquad\sum_{\boldsymbol{s}_u\in\mathcal{S}^M}\left(\frac{P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})}{\sum_{\boldsymbol{s}_p\in\mathcal{S}^M} P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\tilde{\boldsymbol{s}}=\boldsymbol{s}_p,\boldsymbol{H})}\log_2\frac{P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})}{\sum_{\boldsymbol{s}_p\in\mathcal{S}^M} P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\tilde{\boldsymbol{s}}=\boldsymbol{s}_p,\boldsymbol{H})}\right) \\
&\quad= M\log_2 q + \frac{1}{q^M}\sum_{\boldsymbol{s}_v\in\mathcal{S}^M}\sum_{\boldsymbol{s}_u\in\mathcal{S}^M}\left(P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})\log_2\frac{P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})}{\sum_{\boldsymbol{s}_p\in\mathcal{S}^M} P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\tilde{\boldsymbol{s}}=\boldsymbol{s}_p,\boldsymbol{H})}\right).
\end{aligned}
\tag{B.1}
$$

When PSK symbols are transmitted, since the noise is signal-independent and the PSK symbols are equivalent to each other, we have

$$
P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H}) = P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_u|\boldsymbol{s}=\boldsymbol{s}_v,\boldsymbol{H}), \tag{B.2}
$$

which means

$$
\sum_{\boldsymbol{s}_p\in\mathcal{S}^M} P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\tilde{\boldsymbol{s}}=\boldsymbol{s}_p,\boldsymbol{H}) = \sum_{\boldsymbol{s}_p\in\mathcal{S}^M} P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_p|\tilde{\boldsymbol{s}}=\boldsymbol{s}_v,\boldsymbol{H}) = 1. \tag{B.3}
$$

By plugging (B.3) into (B.1) and exchanging the summation order, (4.8) is proved.

## B.2 Proof of Lemma 4.2.2

Given the model in (2.3), when the transmitted vector $\boldsymbol{s} = \boldsymbol{s}_u$, we have

$$\begin{aligned} P\left(\|\boldsymbol{x} - \boldsymbol{s}_v\|^2_{\boldsymbol{W}^{-1}} \le \|\boldsymbol{x} - \boldsymbol{s}_u\|^2_{\boldsymbol{W}^{-1}}\right) &= P\left(\|\boldsymbol{e}_{uv} + \boldsymbol{\eta}\|^2_{\boldsymbol{W}^{-1}} \le \|\boldsymbol{\eta}\|^2_{\boldsymbol{W}^{-1}}\right) \\ &= P\left(\|\boldsymbol{\eta}\|^2_{\boldsymbol{W}^{-1}} + \|\boldsymbol{e}_{uv}\|^2_{\boldsymbol{W}^{-1}} + \boldsymbol{e}_{uv}^{\mathcal{H}}\boldsymbol{W}^{-1}\boldsymbol{\eta} + \boldsymbol{\eta}^{\mathcal{H}}\boldsymbol{W}^{-1}\boldsymbol{e}_{uv} \le \|\boldsymbol{\eta}\|^2_{\boldsymbol{W}^{-1}}\right) \\ &= P\left(\boldsymbol{e}_{uv}^{\mathcal{H}}\boldsymbol{W}^{-1}\boldsymbol{\eta} + \boldsymbol{\eta}^{\mathcal{H}}\boldsymbol{W}^{-1}\boldsymbol{e}_{uv} \le -\|\boldsymbol{e}_{uv}\|^2_{\boldsymbol{W}^{-1}}\right) \end{aligned} \tag{B.4}$$

where $\boldsymbol{e}_{uv} = \boldsymbol{s}_u - \boldsymbol{s}_v$. Since $\boldsymbol{\eta}$ is complex Gaussian distributed with zero mean and covariance matrix $\boldsymbol{W}$, the random variable $\boldsymbol{e}_{uv}^{\mathcal{H}}\boldsymbol{W}^{-1}\boldsymbol{\eta} + \boldsymbol{\eta}^{\mathcal{H}}\boldsymbol{W}^{-1}\boldsymbol{e}_{uv}$ is also complex Gaussian with the mean and variance calculated by

$$E[\boldsymbol{e}_{uv}^{\mathcal{H}}\boldsymbol{W}^{-1}\boldsymbol{\eta} + \boldsymbol{\eta}^{\mathcal{H}}\boldsymbol{W}^{-1}\boldsymbol{e}_{uv}] = \boldsymbol{e}_{uv}^{\mathcal{H}}\boldsymbol{W}^{-1}E[\boldsymbol{\eta}] + E[\boldsymbol{\eta}^{\mathcal{H}}]\boldsymbol{W}^{-1}\boldsymbol{e}_{uv} = 0, \tag{B.5}$$

and

$$\begin{aligned} E\left[(\boldsymbol{e}_{uv}^{\mathcal{H}}\boldsymbol{W}^{-1}\boldsymbol{\eta} + \boldsymbol{\eta}^{\mathcal{H}}\boldsymbol{W}^{-1}\boldsymbol{e}_{uv})^2\right] &= 2\boldsymbol{e}_{uv}^{\mathcal{H}}\boldsymbol{W}^{-1}E[\boldsymbol{\eta}^{\mathcal{H}}\boldsymbol{\eta}]\boldsymbol{W}^{-1}\boldsymbol{e}_{uv} \\ &= 2\boldsymbol{e}_{uv}^{\mathcal{H}}\boldsymbol{W}^{-1}\boldsymbol{W}\boldsymbol{W}^{-1}\boldsymbol{e}_{uv} \\ &= 2\boldsymbol{e}_{uv}^{\mathcal{H}}\boldsymbol{W}^{-1}\boldsymbol{e}_{uv}. \end{aligned} \tag{B.6}$$

Hence, $\boldsymbol{e}_{uv}^{\mathcal{H}}\boldsymbol{W}^{-1}\boldsymbol{\eta}+\boldsymbol{\eta}^{\mathcal{H}}\boldsymbol{W}^{-1}\boldsymbol{e}_{uv}$ is Gaussian distributed with zero mean and variance $2\boldsymbol{e}_{uv}^{\mathcal{H}}\boldsymbol{W}^{-1}\boldsymbol{e}_{uv}$. Back to (B.4), we have (4.12) which is the conclusion of lemma 4.2.2.

## B.3 Proof of Lemma 4.2.3

Denote $D(v,k|u) = \|\boldsymbol{x} - \boldsymbol{s}_v\|^2_{\boldsymbol{W}^{-1}} - \|\boldsymbol{x} - \boldsymbol{s}_k\|^2_{\boldsymbol{W}^{-1}}$ provided that $\boldsymbol{s} = \boldsymbol{s}_u$. Substituting $D(v,k|u)$ in (4.9), the error probability is

$$\begin{aligned} &P(\hat{\boldsymbol{s}}_{ML} = \boldsymbol{s}_v|\boldsymbol{s} = \boldsymbol{s}_u, u \ne v, \boldsymbol{H}) \\ &= P\left(D(v,k|u) \le 0, \quad \forall k\right) \\ &= P\left(D(v,u|u) \le 0\right) \cdot P\left(D(v,k|u) \le 0 | D(v,u|u) \le 0, \forall k \ne v \text{ and } k \ne u\right) \\ &= Q\Big(\frac{\sigma_{ML}(uv)}{2}\Big) \cdot P\left(D(v,k|u) \le 0 | D(v,u|u) \le 0, \forall k \ne v \text{ and } k \ne u\right), \end{aligned} \tag{B.7}$$

where the final step is obtained via (4.12) presented in lemma 4.2.2. Since the second term in (B.7) is less than or equal to 1, the conclusion of lemma 4.2.3 holds.

## B.4 Proof of Theorem 4.2.5

In this appendix, we show how to derive the lower bound of PMI with MLD for PSK symbols. When PSK symbols are employed, the PMI with MLD is given by (4.8):

$$\begin{aligned}
&\mathcal{I}(\boldsymbol{s};\hat{\boldsymbol{s}}_{ML}|\boldsymbol{H}) \\
&= M\log_2 q + \frac{1}{q^M}\sum_{\boldsymbol{s}_u\in\mathcal{S}^M}\sum_{\boldsymbol{s}_v\in\mathcal{S}^M}\left(P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})\cdot\log_2 P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})\right) \\
&= M\log_2 q - \frac{1}{q^M}\sum_{\boldsymbol{s}_u\in\mathcal{S}^M}\mathcal{H}(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u),
\end{aligned} \tag{B.8}$$

where

$$\mathcal{H}(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u) = \sum_{\boldsymbol{s}_v\in\mathcal{S}^M}\left(P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})\cdot\log_2 P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})\right). \tag{B.9}$$

Notice that $\mathcal{H}(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u)$ is an entropy function which achieves its maximum value if and only if $P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})=\frac{1}{|\mathcal{S}|^M}$ for any $\boldsymbol{s}_v\in\mathcal{S}^M$. Furthermore, according to the characteristics of the entropy function, the more uniform $P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})$ is, the larger $\mathcal{H}(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u)$ is. We prove the conclusion of Theorem 4.2.5 in the following three steps.

Step 1: Consider the signal set $\mathcal{S}_1^M=\{\boldsymbol{s}_{l1(1)},\boldsymbol{s}_{l1(2)},\cdots\}\subseteq\mathcal{S}^M\setminus\{\boldsymbol{s}_u\}$. Each symbol in $\mathcal{S}_1^M$ satisfies $Q\Big(\frac{\sigma_{ML}(ul1(\cdot))}{2}\Big)\leq\frac{1}{|\mathcal{S}|^M}$, where $l1(\cdot)$ represents any index in the set $\{l1(1),l1(2),\cdots\}$. Via the claims in Lemma 4.2.3 and Lemma 4.2.4, we have

$$P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_{l1(\cdot)}|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})\leq Q\Big(\frac{\sigma_{ML}(ul1(\cdot))}{2}\Big)\leq\frac{1}{|\mathcal{S}|^M},\text{ and} \tag{B.10}$$

$$P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_u|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})\geq 1-\sum_{\boldsymbol{s}_{l1(\cdot)}\in\mathcal{S}_1^M}Q\Big(\frac{\sigma_{ML}(ul1(\cdot))}{2}\Big)\geq\frac{1}{|\mathcal{S}|^M}. \tag{B.11}$$

Now we use $Q\Big(\frac{\sigma_{ML}(ul1(\cdot))}{2}\Big)$ to replace the true error probabilities of these signals and use $1-\sum_{\boldsymbol{s}_{l1(\cdot)}\in\mathcal{S}_1^M}Q\Big(\frac{\sigma_{ML}(ul1(\cdot))}{2}\Big)$ to replace the true correct detection probability to estimate $\mathcal{H}(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u)$. We denote the estimated one as $\hat{\mathcal{H}}(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u)$. Notice that the difference between the replaced error and correct detection probabilities is smaller than the true difference between

them, but the error probabilities and the correct detection probability are still on the two sides of $\frac{1}{|\mathcal{S}|^M}$. From the characteristics of the entropy function, we have

$$\hat{\mathcal{H}}(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u) > \mathcal{H}(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u). \tag{B.12}$$

Eq.(B.12) shows that if we use the upper bound of the error probabilities for the signals in $\mathcal{S}_1^M$ to replace the real values of them and use the lower bound of the correction detection probability to replace the true value, then the estimated $\hat{\mathcal{H}}(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u)$ is larger than the true value. This conclusion is consistent with the claim in theorem 1. Therefore, in the following we do not need to consider the signals in $\mathcal{S}_1^M$, we focus on the symbols which are not in $\mathcal{S}_1^M$.

Step 2: denote

$$\begin{aligned}&\mathcal{H}_1(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u) \\ &= \mathcal{H}(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u) - \sum_{\boldsymbol{s}_v\in\mathcal{S}_1^M}\left(P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})\cdot\log_2 P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})\right).\end{aligned} \tag{B.13}$$

From the definition of $\mathcal{H}_1(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u)$, we can conclude that $\mathcal{H}_1(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u)$ is still an entropy-like function but with the sum of the probabilities $1-\sum_{\boldsymbol{s}_v\in\mathcal{S}_1^M} P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})$ instead of 1. Similar to the entropy function, $\mathcal{H}_1(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u)$ achieves its maximum value when

$$P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v,\ \boldsymbol{s}_v\in\mathcal{S}^M\setminus\mathcal{S}_1^M|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H}) = \frac{1-\sum_{\boldsymbol{s}_v\in\mathcal{S}_1^M} P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})}{|\mathcal{S}^M\setminus\mathcal{S}_1^M|}. \tag{B.14}$$

Let $\mathcal{S}_2^M=\{\boldsymbol{s}_{l2(1)},\boldsymbol{s}_{l2(2)},\cdots\}\subseteq\mathcal{S}^M\setminus\{\mathcal{S}_1^M\bigcup\{\boldsymbol{s}_u\}\}$ each signal of which satisfies $Q\left(\frac{\sigma_{ML}(ul2(\cdot))}{2}\right)\leq \frac{1}{|\mathcal{S}^M\setminus\mathcal{S}_1^M|}\left(1-\sum_{\boldsymbol{s}_v\in\mathcal{S}_1^M} P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})\right)$. Similar to Step 1, we have

$$\hat{\mathcal{H}}_1(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u) \geq \mathcal{H}_1(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u), \tag{B.15}$$

where

$$\hat{\mathcal{H}}_1(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u)=\Bigg[\sum_{\boldsymbol{s}_{l2(\cdot)}\in\mathcal{S}_2^M} Q\Big(\frac{\sigma_{ML}(ul2(\cdot))}{2}\Big)\log_2 Q\Big(\frac{\sigma_{ML}(ul2(\cdot))}{2}\Big)$$
$$+\left(1-\sum_{\boldsymbol{s}_v\in\mathcal{S}_1^M} P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})-\sum_{\boldsymbol{s}_{l2(\cdot)}\in\mathcal{S}_2^M} Q\Big(\frac{\sigma_{ML}(ul2(\cdot))}{2}\Big)\right)$$
$$\cdot\log_2\left(1-\sum_{\boldsymbol{s}_v\in\mathcal{S}_1^M} P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})-\sum_{\boldsymbol{s}_{l2(\cdot)}\in\mathcal{S}_2^M} Q\Big(\frac{\sigma_{ML}(ul2(\cdot))}{2}\Big)\right)\Bigg]. \quad \text{(B.16)}$$

Next, let

$$\mathcal{H}_2(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u) \quad \text{(B.17)}$$
$$=\mathcal{H}_1(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u)-\sum_{\boldsymbol{s}_v\in\mathcal{S}_2^M}\left(P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})\cdot\log_2 P(\hat{\boldsymbol{s}}_{ML}=\boldsymbol{s}_v|\boldsymbol{s}=\boldsymbol{s}_u,\boldsymbol{H})\right).$$

Step 3: repeat Step 1 and Step 2 until all the symbols in $\mathcal{S}^M\setminus\{\boldsymbol{s}_u\}$ are partitioned in different subsets $\boldsymbol{S}_p^M$.

Summarizing the results from Step 1 to 3, we have shown that any increase in the error probabilities and the corresponding decrease in the correct detection probability induce the increase of $\mathcal{H}(\hat{\boldsymbol{s}}_{ML}|\boldsymbol{s}=\boldsymbol{s}_u)$. Combining the conclusion with (B.8), theorem 4.2.5 is proved.

## B.5 Proof of Lemma 4.3.2

First we assume $\hat{\boldsymbol{s}}_{ZF}=\boldsymbol{s}_v$. From (4.5) we have

$$\|x_m-s_{v,m}\|^2\le\|x_m-s_{k,m}\|^2 \quad \text{(B.18)}$$

for $m=1,\cdots,M$ and $\forall k\neq v$. It is straight forward to obtain

$$(\boldsymbol{x}-\boldsymbol{s}_v)^\dagger\boldsymbol{\Lambda}(\boldsymbol{x}-\boldsymbol{s}_v)=\sum_{m=1}^{M}\Lambda_{m,m}\|x_m-s_{v,m}\|^2$$
$$\le\sum_{m=1}^{M}\Lambda_{m,m}\|x_m-s_{k,m}\|^2$$
$$=(\boldsymbol{x}-\boldsymbol{s}_k)^\dagger\boldsymbol{\Lambda}(\boldsymbol{x}-\boldsymbol{s}_k), \quad \text{(B.19)}$$

for $\forall k \neq v$. On the other hand, let

$$\boldsymbol{s}_v = \arg\min_{\tilde{\boldsymbol{s}} \in \mathcal{S}^M} (\boldsymbol{x} - \tilde{\boldsymbol{s}})^\dagger \boldsymbol{\Lambda} (\boldsymbol{x} - \tilde{\boldsymbol{s}}). \tag{B.20}$$

If there exists $s_{k,n} \in \mathcal{S}$ and $s_{k,n} \neq s_{v,n}$ such that $\|x_n - s_{k,n}\|^2 < \|x_n - s_{v,n}\|^2$, then there should be $\boldsymbol{s}_k \in \mathcal{S}^M$ which is defined by

$$\begin{cases} s_{k,m} = s_{k,n} & \text{if } m = n \\ s_{k,m} = s_{v,m} & \text{if } m \neq n \text{ and } m = 1, \cdots, M. \end{cases} \tag{B.21}$$

Hence we have

$$\begin{aligned} &(\boldsymbol{x} - \boldsymbol{s}_v)^\dagger \boldsymbol{\Lambda} (\boldsymbol{x} - \boldsymbol{s}_v) - (\boldsymbol{x} - \boldsymbol{s}_k)^\dagger \boldsymbol{\Lambda} (\boldsymbol{x} - \boldsymbol{s}_k) \\ &\qquad = \sum_{m=1}^{M} \Lambda_{m,m} \|x_m - s_{v,m}\|^2 - \sum_{m=1}^{M} \Lambda_{m,m} \|x_m - s_{k,m}\|^2 \\ &\qquad = \Lambda_{n,n} (\|x_n - s_{v,n}\|^2 - \|x_n - s_{k,n}\|^2) > 0. \end{aligned} \tag{B.22}$$

This is contradicted with (B.20). Therefore there is no such $s_{k,n}$. Hence lemma 4.3.2 is proved.

## B.6 Proof of Lemma 4.3.6

According to (2.3) and (4.3), we have

$$\begin{aligned} \boldsymbol{x} &= \boldsymbol{s} + \boldsymbol{H}^\dagger \boldsymbol{\omega} \\ &= [Re(\boldsymbol{s}) + iIm(\boldsymbol{s})] + [Re(\boldsymbol{H}^\dagger) + iIm(\boldsymbol{H}^\dagger)][Re(\boldsymbol{\omega}) + iIm(\boldsymbol{\omega})] \\ &= [Re(\boldsymbol{s}) + \boldsymbol{A}Re(\boldsymbol{\omega}) - \boldsymbol{B}Im(\boldsymbol{\omega})] + i\,[Im(\boldsymbol{s}) + \boldsymbol{A}Im(\boldsymbol{\omega}) + \boldsymbol{B}Re(\boldsymbol{\omega})] \end{aligned} \tag{B.23}$$

which is equivalent to

$$\begin{aligned} \boldsymbol{z} = \begin{bmatrix} Re(\boldsymbol{x}) \\ Im(\boldsymbol{x}) \end{bmatrix} &= \begin{bmatrix} Re(\boldsymbol{s}) \\ Im(\boldsymbol{s}) \end{bmatrix} + \begin{bmatrix} \boldsymbol{A}Re(\boldsymbol{\omega}) - \boldsymbol{B}Im(\boldsymbol{\omega}) \\ \boldsymbol{A}Im(\boldsymbol{\omega}) + \boldsymbol{B}Re(\boldsymbol{\omega}) \end{bmatrix} \\ &= \begin{bmatrix} Re(\boldsymbol{s}) \\ Im(\boldsymbol{s}) \end{bmatrix} + \begin{bmatrix} \boldsymbol{A} & -\boldsymbol{B} \\ \boldsymbol{B} & \boldsymbol{A} \end{bmatrix} \begin{bmatrix} Re(\boldsymbol{\omega}) \\ Im(\boldsymbol{\omega}) \end{bmatrix}. \end{aligned} \tag{B.24}$$

From (B.24), the covariance matrix of $\boldsymbol{z}$ is given by

$$E[\boldsymbol{z}\boldsymbol{z}^T] = E\left[\begin{bmatrix} \boldsymbol{A} & -\boldsymbol{B} \\ \boldsymbol{B} & \boldsymbol{A} \end{bmatrix}\begin{bmatrix} Re(\boldsymbol{\omega}) \\ Im(\boldsymbol{\omega}) \end{bmatrix}\begin{bmatrix} Re(\boldsymbol{\omega})^T & Im(\boldsymbol{\omega})^T \end{bmatrix}\begin{bmatrix} \boldsymbol{A}^T & \boldsymbol{B}^T \\ -\boldsymbol{B}^T & \boldsymbol{A}^T \end{bmatrix}\right]$$
$$= \begin{bmatrix} \boldsymbol{A} & -\boldsymbol{B} \\ \boldsymbol{B} & \boldsymbol{A} \end{bmatrix} E\left[\begin{bmatrix} Re(\boldsymbol{\omega}) \\ Im(\boldsymbol{\omega}) \end{bmatrix}\begin{bmatrix} Re(\boldsymbol{\omega})^T & Im(\boldsymbol{\omega})^T \end{bmatrix}\right]\begin{bmatrix} \boldsymbol{A}^T & \boldsymbol{B}^T \\ -\boldsymbol{B}^T & \boldsymbol{A}^T \end{bmatrix}. \quad \text{(B.25)}$$

Since $\boldsymbol{\omega}$ is circular complex white Gaussian noise, we have

$$E\left[\begin{bmatrix} Re(\boldsymbol{\omega}) \\ Im(\boldsymbol{\omega}) \end{bmatrix}\begin{bmatrix} Re(\boldsymbol{\omega})^T & Im(\boldsymbol{\omega})^T \end{bmatrix}\right] = \sigma_\omega^2\begin{bmatrix} \boldsymbol{I}_{M\times M} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{I}_{M\times M} \end{bmatrix} \quad \text{(B.26)}$$

Combining (B.26) with (B.25) proves the claim in lemma 4.3.6.

## B.7 Proof of Theorem 4.4.1

If $od(\boldsymbol{H}) = 0$, then $\boldsymbol{H}$ is an orthogonal matrix. Therefore, the covariance matrix of the equalized vector $\boldsymbol{W}$ given in (4.4) is a diagonal matrix. According to (4.9) and (4.32), when we choose $\boldsymbol{\Lambda} = \boldsymbol{W}$, we have

$$P\{\hat{\boldsymbol{s}}_{ZF} = \boldsymbol{s}_v | \boldsymbol{s} = \boldsymbol{s}_u, u \neq v, \boldsymbol{H}\} = P\{\hat{\boldsymbol{s}_{ML}} = \boldsymbol{s}_v | \boldsymbol{s} = \boldsymbol{s}_u, u \neq v, \boldsymbol{H}\} \quad \text{(B.27)}$$

where $\hat{\boldsymbol{s}}$ is the detected vector with MLD. Substituting (B.27) into (4.8) and (4.30) gives us the result of theorem 4.4.1.

# APPENDIX C

# PROOF FOR CHAPTER 5

## C.1 Proof of Lemma 5.4.2

The size of the suspicious set $\mathcal{D}_{s_p}$ should be greater or equal to 1 and less or equal to $M$. Hence, we have

$$1 \leq E\left[|\mathcal{D}_{s_p}|\right] \leq M. \tag{C.1}$$

Let us consider $\mathcal{D}_{s_1}$ first. Notice that when $s_1 \in \mathcal{D}_1$, there still may be some erased random symbols in the first row of $\mathbf{\Gamma}$ that are equal to $s_1$. Under such situation, (5.9) must hold. Thus $s_1$ is successfully mixed with other random symbols. Hence the size of $\mathcal{D}_{s_1}$ is $M$ for this case. For the expectation of the size of $\mathcal{D}_{s_1}$, we have

$$\begin{aligned} E\left[|\mathcal{D}_{s_1}|\right] &\geq P\left(s_1 \in \left\{\gamma_{1,np_l+1},\ \gamma_{1,np_l+2}, \cdots, \gamma_{1,n}\right\}\right) \cdot M \\ &= \left[1 - P\left(s_1 \in \left\{\gamma_{1,np_l+1},\ \gamma_{1,np_l+2}, \cdots, \gamma_{1,n}\right\}\right)\right] \cdot M \\ &= \left[1 - (1 - \frac{1}{M})^{np_e}\right] \cdot M. \end{aligned} \tag{C.2}$$

Combining (C.2) and (5.11), Lemma 5.4.2 is proved.

## C.2 Proof of Lemma 5.4.3

First, let us compute the probability that Eve can successfully decode $s_1$, which is

$$\begin{aligned} P(\hat{s}_1 = s_1|\mathbf{z}) &= P\left(c_1 \in \mathcal{D}_1,\ s_1 \in \mathcal{D}_1\right) \cdot \frac{1}{E\left[|\mathcal{D}_{s_1}|\right]} \\ &\quad + \left[1 - P\left(c_1 \in \mathcal{D}_1,\ s_1 \in \mathcal{D}_1\right)\right] \cdot \frac{1}{M} \\ &= \frac{P_{n-2}^{n-2} P_{p_l n}^2}{P_n^n} \cdot \frac{1}{E\left[|\mathcal{D}_{s_1}|\right]} + \frac{P_n^n - P_{n-2}^{n-2} P_{p_l n}^2}{P_n^n} \cdot \frac{1}{M} \\ &\leq \frac{P_{n-2}^{n-2} P_{p_l n}^2}{P_n^n} \cdot \frac{1}{A} + \frac{P_n^n - P_{n-2}^{n-2} P_{p_l n}^2}{P_n^n} \cdot \frac{1}{M}. \end{aligned} \tag{C.3}$$

The last inequality in (C.3) is derived from (5.13).

The probability that Eve can successfully decode each symbol of $\boldsymbol{s}$ is independent of each other, thus we have

$$
\begin{aligned}
P(\hat{\boldsymbol{s}} = \boldsymbol{s}|\boldsymbol{z}) &= \prod_{p=1}^{m} P(\hat{s}_p = s_p|\boldsymbol{z}) \\
&= [P(\hat{s}_1 = s_1|\boldsymbol{z})]^m \\
&= \left[ \frac{P_{n-2}^{n-2} P_{p_l n}^2}{P_n^n} \cdot \frac{1}{E\left[|\mathcal{D}_{s_1}|\right]} + \frac{P_n^n - P_{n-2}^{n-2} P_{p_l n}^2}{P_n^n} \cdot \frac{1}{M} \right]^m \qquad \text{(C.4)} \\
&\leq \left[ \frac{(P_{n-2}^{n-2} P_{p_l n}^2)^{\frac{1}{A}} + (P_n^n - P_{n-2}^{n-2} P_{p_l n}^2)^{\frac{1}{M}}}{P_n^n} \right]^m . \qquad \text{(C.5)}
\end{aligned}
$$

## C.3 Proof of Lemma 5.4.4

When $\frac{m}{n} \leq p_e$, we have the following inequations:

$$
\begin{aligned}
\left[1 - (1 - \frac{1}{M})^{np_e}\right]^{np_e} &\leq \left[1 - (1 - \frac{1}{M})^{np_e}\right]^{i} \\
&< \left[1 - (1 - \frac{1}{M})^{np_e}\right]^{0}, \qquad \text{(C.6)}
\end{aligned}
$$

for $i = 1, \cdots, m$. The right term in (C.6) is equal to 1. As for the left term, we have

$$
\log\left[1 - (1 - \frac{1}{M})^{np_e}\right]^{np_e} = \frac{\log\left[1 - (1 - \frac{1}{M})^{np_e}\right]}{\frac{1}{np_e}} \to 0 \qquad \text{(C.7)}
$$

as $n \to \infty$, thus $\left[1 - (1 - \frac{1}{M})^{np_e}\right]^{np_e} \to 1$. Since both the lower and the upper bounds converge to 1, then

$$
\left[1 - (1 - \frac{1}{M})^{np_e}\right]^{i} \to 1 \text{ as } n \to \infty, \qquad \text{(C.8)}
$$

for $i = 1, \cdots, m$.

## C.4 Proof of Theorem 5.4.7

Suppose there are $m - k$ rows of $\boldsymbol{\Gamma}$ in which both the confidential symbols $s_p$ and the check symbols $c_p$ are in the first $np_l$ symbols, *i.e.,* Eve will apply the second step of the decoding strategy to decode the $m - k$ symbols in $\boldsymbol{s}$. Denote the set of the observations of Eve $\boldsymbol{z}'s$ that are generated by such $\boldsymbol{\Gamma}$ as $Q_k$. When the observation of Eve $\boldsymbol{z} \in Q_k$, the number of

the possible $m-k$ confidential symbols that can generate such $\boldsymbol{z}$ is equal to $(E[|\mathcal{D}_{s_1}|])^{m-k}$. Except for the $m-k$ rows, there should be $k$ rows of $\boldsymbol{\Gamma}$ in which the confidential symbol and the check symbol are not both in the first $np_l$ symbols. Denote the set of the observations of Eve $\boldsymbol{z}'s$ that are generated by such $\boldsymbol{\Gamma}$ as $\mathcal{R}_k$. According to (5.12), when the observation of Eve $\boldsymbol{z} \in \mathcal{R}_k$, the number of the possible $k$ confidential symbols that can generate such $\boldsymbol{z}$ is equal to $M^k$. Hence we have:

$$\begin{aligned}
&\mathcal{H}(\boldsymbol{s}|\boldsymbol{z} \in \mathcal{Q}_k \cap \mathcal{R}_k) \\
&= P(\boldsymbol{z} \in \mathcal{Q}_k \cap \mathcal{R}_k) \cdot \log_2 \left( M^k \times (E[|\mathcal{D}_{s_1}|])^{m-k} \right) \\
&= \binom{m}{k} \frac{(P_{n-2}^{n-2} P_{p_l n}^2)^{m-k} (P_n^n - P_{n-2}^{n-2} P_{p_l n}^2)^k}{(P_n^n)^m} \\
&\qquad \cdot \log_2 \left( M^k \times (E[|\mathcal{D}_{s_1}|])^{m-k} \right) \\
&\geq \binom{m}{k} \frac{(P_{n-2}^{n-2} P_{p_l n}^2)^{m-k} (P_n^n - P_{n-2}^{n-2} P_{p_l n}^2)^k}{(P_n^n)^m} \\
&\qquad \cdot \log_2 \left( M^k \times A^{m-k} \right), \qquad \text{(C.9)}
\end{aligned}$$

where the last inequality is derived from (5.13). Since $k$ can be 0 to $m$, thus

$$\begin{aligned}
\mathcal{H}(\boldsymbol{s}|\boldsymbol{z}) &= \sum_{k=0}^{m} \mathcal{H}(\boldsymbol{s}|\boldsymbol{z} \in \mathcal{Q}_k \cap \mathcal{R}_k) \\
&= \sum_{k=0}^{m} \binom{m}{k} \frac{(P_{n-2}^{n-2} P_{p_l n}^2)^{m-k} (P_n^n - P_{n-2}^{n-2} P_{p_l n}^2)^k}{(P_n^n)^m} \\
&\qquad \cdot \log_2 \left( M^k \times (E[|\mathcal{D}_{s_1}|])^{m-k} \right) \\
&\geq \sum_{k=0}^{m} \binom{m}{k} \frac{(P_{n-2}^{n-2} P_{p_l n}^2)^{m-k} (P_n^n - P_{n-2}^{n-2} P_{p_l n}^2)^k}{(P_n^n)^m} \\
&\qquad \cdot \log_2 \left( M^k \times A^{m-k} \right). \qquad \text{(C.10)}
\end{aligned}$$

Via (C.10), we have

$$\begin{aligned}
R_{NS} &= \frac{\mathcal{H}(\boldsymbol{s}|\boldsymbol{z})}{\mathcal{H}(\boldsymbol{s})} \\
&\geq \frac{1}{m \log_2 M} \sum_{k=0}^{m} \binom{m}{k} \frac{(P_{n-2}^{n-2} P_{p_l n}^2)^{m-k} (P_n^n - P_{n-2}^{n-2} P_{p_l n}^2)^k}{(P_n^n)^m} \\
&\qquad \cdot \log_2 (M^k \cdot A^{m-k}). \qquad \text{(C.11)}
\end{aligned}$$

## C.5 Proof of Corollary 5.4.8

With fixed $p_e$, when $m/n \leq p_e$ and $n \to \infty$, via (5.15), $A \to M$. From (C.11) and the result of Lemma 3, we have

$$
\begin{aligned}
& R_{NS} \\
& \geq \frac{1}{m \log_2 M} \binom{m}{k} \cdot \sum_{k=0}^{m} \frac{(P_{n-2}^{n-2} P_{p_l n}^2)^{m-k} (P_n^n - P_{n-2}^{n-2} P_{p_l n}^2)^k}{(P_n^n)^m} \\
& \qquad \cdot \log_2 (M^k \cdot A^{m-k}) \\
& \to \frac{1}{m \log_2 M} \binom{m}{k} \cdot \sum_{k=0}^{m} \frac{(P_{n-2}^{n-2} P_{p_l n}^2)^{m-k} (P_n^n - P_{n-2}^{n-2} P_{p_l n}^2)^k}{(P_n^n)^m} \\
& \qquad \cdot \log_2 M^m \\
& = \frac{1}{m \log_2 M} \cdot \log_2 M^m \cdot \left( \frac{P_{n-2}^{n-2} P_{p_l n}^2 + P_n^n - P_{n-2}^{n-2} P_{p_l n}^2}{P_n^n} \right)^m \\
& = 1. \qquad \text{(C.12)}
\end{aligned}
$$

By the definition of the normalized security information rate, $R_{NS}$ should be less than or equal to 1. Limited by both the upper bound and the lower bound, $R_{NS}$ converges to 1 as $n \to \infty$.

# REFERENCES


[1] M. H. DeGroot, *Optimal statistical decisions*. Wiley-interscience, 2004.

[2] J. Choi, "On the partial map detection with applications to mimo channels," *IEEE Trans. Signal Processing*, vol. 53, pp. 158–167, 2005.

[3] B. D. Hart and S. Pasupathy, "Innovations-based map detection for time-varying frequency-selective channels," *IEEE Trans. Commun.*, vol. 48, pp. 1507–1019, 2002.

[4] M. O. Damen, H. El Gamal and G. Caire, "On maximum-likelihood detection and the search for the closest lattice point," *IEEE Trans. Inf. Theory.*, vol. 49, pp. 2389–2402, 2003.

[5] X. Zhu and R. D. Murch, "Performance analysis of maximum likelihood detection in a mimo antenna system," *IEEE Trans. Commun.*, vol. 50, pp. 187–191, 2002.

[6] L. Li and A. J. Goldsmith, "Low-complexity maximum-likelihood detection of coded signals sent over finite-state markov channels," *IEEE Trans. Commun.*, vol. 50, pp. 524–531, 2002.

[7] J. G. Proakis, *Digital communications*. McGraw-Hill, 2001.

[8] G. J. Foschini and M. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," *Wireless Personal Commun.*, vol. 6, pp. 311–335, 1998.

[9] I. E. Telatar, "Capacity of multi-antenna Gaussian channels," *Europ. Trans. Telecommun*, vol. 10, no. 6, pp. 586–595, 1999.

[10] G. G. Raleigh and J. M. Cioffi, "Spatio-temporal coding for wireless communication," vol. 46, pp. 357–366, Mar. 1998.

[11] H. Liu, "Error performance of mimo systems in frequency-selective rayleigh fading channels," in *in Proc. IEEE Global Telecommun. Conf.*, (San Francisco, CA), p. 2104C2108, 2003.

[12] J. Winters, "On the capacity of radio communication systems with diversity in a rayleigh fading environment," vol. 5, pp. 871–878, June 1987.

[13] D. N. C. Tse and P. Viswanath, *Fundamentals of wireless communications*. Cambridge, U. K.: Cambridge Univ. Press, 2005.

[14] A. Goldsmith, S. Jafar, N. Jindal, and S. Vishwanath, "Capacity limits of MIMO channels," vol. 21, no. 5, pp. 684–702, 2003.

[15] E. Visotsky and U. Madhow, "Space-time transmit precoding with imperfect feedback," vol. 47, pp. 2632–2639, Sept. 2001.

[16] A. Narula, M. Trott, and G. Wornel, "Performance limits of coded diversity methods for transmitter antenna arrays," vol. 45, pp. 2418–2433, Nov. 1999.

[17] S. Jafar and A. Goldsmith, "Transmitter optimization and optimality of beamforming for multiple antenna systems," vol. 3, pp. 1165–1175, July 2004.

[18] E. Jorswieck and H. Boche, "Channel capacity and capacity-range of beamforming in MIMO wireless systems under correlated fading with covariance feedback," vol. 3, pp. 1543–1553, Sept. 2004.

[19] S. Simon and A. Moustakas, "Optimizing MIMO antenna systems with channel covariance feedback," vol. 21, pp. 406–417, Apr. 2003.

[20] M. Kiessling and J. Speidel, "Analytical performance of MIMO zero-forcing receivers in correlated Rayleigh fading environments," in *Proc. IEEE Workshop Signal Process. Adv. Wireless Commun.*, (Rome, Italy), pp. 383–387, 2003.

[21] D. Gore, R. Heath, and A. Paulraj, "Transmit selection in spatial multiplexing systems," vol. 6, pp. 491–493, Nov. 2002.

[22] H. Liu, "Error performance of MIMO systems in frequency-selective rayleigh fading channels," in *Proc. IEEE Global Telecommun. Conf.*, vol. 4, (San Francisco, CA), pp. 2104–2108, Dec. 2003.

[23] S. H. Muller-Weinfurtner, "Coding approaches for multiple antenna transmission in fast fading and OFDM," vol. 50, pp. 2442–2450, Oct. 2002.

[24] X. Zhu and R. D. Murch, "Performance analysis of maximum likelihood detection in a MIMO antenna system," vol. 50, pp. 187–191, Feb. 2002.

[25] N. G. M. Sling, J. Speidel and M. Reinhardt, "Performance analysis of MIMO maximum likelihood receivers with channel correlation, colored gaussian noise, and linear prefiltering," in *in Proc. IEEE International Conf. on Communications*, (Anchorage, AK), pp. 3026 – 3030, 2003.

[26] C.-J. Chen and L.-C. Wang, "On the performance of the zero-forcing reciever operating in the multiuser mimo sytem with reduced noise enhancement effect," in *Proc. IEEE Global Telecommun. Conf.*, vol. 3, (St. Louis, MO), pp. 1294–1298, Nov. 2005.

[27] H. Shin and J. H. Lee, "Capacity of multiple-antanna fading channels:spatial fading correlation, double scattering, and keyhole," vol. 49, pp. 2636–2647, Oct. 2003.

[28] X. Ma and W. Zhang, "Fundamental limits of linear Equalizers: Diversity, capacity, and complexity," vol. 54, pp. 3442–3456, Aug. 2008.

[29] M. R. McKay and I. B. Collings, "Capacity and performance of MIMO-BICM with zero-forcing receivers," vol. 53, pp. 74–83, Jan. 2005.

[30] M. Kiessling and J. Speidel, "Analytical performance of mimo zeroforcing receivers in correlated rayleigh fading environments," in *in Proc. IEEE Workshop Signal Process. Adv. Wireless Commun.*, (Rome, Italy), p. 383C387, 2003.

[31] A. D. Wyner, "The wiretap channel," *Bell. Syst. Tech. Journal*, vol. 54, pp. 1355–1387, October 1975.

[32] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J. M. Merolla, "Applications of LDPC codes to the wiretap channel," vol. 53, no. 8, pp. 2933–2945, 2007.

[33] X. M. J. Xiao and S. W. McLaughlin, "Random complex field code design for security over wiretap channels," in *in Proc. Annual Conference on Information Sciences and Systems*, (Baltimore, MD), 2011.

[34] J. Ashley, et al., "Holographic data storage," *IBM J. Res. Dev.*, vol. 44, pp. 341–368, May 2000.

[35] M. Keskinoz and B.V. K. Vijaya Kumar, "Discrete magnitude-squared channel modeling, equalization, and detection for volume holographic storage channels," *Applied Optics*, vol. 43, pp. 1368–1378, Feb. 2004.

[36] B. M. King and M. A. Neifeld, "Parallel detection algorithm for page-oriented optical memories," *Applied Optics*, vol. 37, pp. 6275–6298, 1998.

[37] C. Moster, B. Schupp, and D. Psaltis, "Localized holographic recording in doubly doped lithium niobate," *Optics Letters*, vol. 25, pp. 162–164, Feb. 2000.

[38] A. Karbaschi, O. Momtahan, and A. Adibi, "Dynamic optical correlation using localized holography," *Optics Letters*, vol. 32, pp. 597–599, Feb. 2007.

[39] S.G. Srinivasa, O. Momtahan, A. Karbaschi, S. W. McLaughlin, A. Adibi, and F. Fekri, "M-ary, binary, and space-volume multiplexing trade-offs for holographic channels," in *Proc. IEEE Global Telecomm. Conf.*, (San Francisco, USA), pp. 1–5, Nov. 2006.

[40] L. R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. Inf. Theory.*, vol. 20, pp. 284–287, 1974.

[41] Jordan, R. ; Host, S. ; Johannesson, R. ; Bossert, M. ; Zyablov, V.V., "Woven convolutional codes. II: decoding aspects," *IEEE Trans. Inf. Theory.*, vol. 50, pp. 2522–2531, Oct. 2004.

[42] C. Wu , M. Shieh and C. Wu, "Memory arrangements in turbo decoders using sliding-window BCJR algorithm," in *IEEE International Symposium on Circuits and Systems*, (Scottsdale, Arizona), pp. 557–560, May 2002.

[43] J. B. Soriaga, P. H. Siegel, and J. K. Wolf, "On achievable rates of multistage decoding on two-dimensional ISI channels," in *Proc. IEEE Int. Symp. Information Theory*, (Adelaide, Austrlia), pp. 1348–1352, 2005.

[44] J. Chen and P. H. Siegel, "On the symmetric information rate of two-dimensional finite-state ISI channels," *IEEE Trans. Inf. Theory.*, vol. 52, pp. 227–236, Jan. 2006.

[45] J. Xiao, A. Karbaschi, A. Adibi and S. W. McLaughlin, "Multilevel coding and multistage decoding for M-ary two-dimensional ISI channels," in *Proc. Conf. on Info. Sciences and Systems*, (Baltimore, U.S.), pp. 77–80, Mar. 2009.

[46] A. Gersho and R. M. Gray, *Vector Quantization and Signal Compression*, ch. 5-6, 10-12. Boston, MA: Kluwer Academic Publishers, 1992.

[47] P. Vogel, "Analytical coding of gaussian sources," vol. 40, pp. 1639–1645, Sept. 1994.

[48] Y. Linde, A. Buzo, and R. Gray, "An algorithm for vector quantizer design," vol. 28, pp. 84–95, Jan. 1980.

[49] G. A. Gray and G. W. Zeoli, "Quantization and saturation noise due to analog-to-digital conversion," pp. 222–223, Jan. 1971.

[50] D. A. Gore, R. W. Heath, Jr, and A. J. Paulraj, "On performance of the zero forcing receiver in presense of transmit correlation," in *Proc. IEEE Int. Symp. Information Theory*, (Lausanne, Switzerland), p. 159, Jun./Jul. 2002.

[51] E. Biglieri, G. Taricco, and E. Viterbo, "Bit-interleaved time-space codes for fading channels," in *Proc. Conf. Inf. Theory*, (Princeton, NJ), pp. WA4.1–WA4.6, 2000.

[52] S. H. Muller-Weinfurtner, "Coding approaches for multiple antenna transmission in fast fading and OFDM," vol. 50, pp. 2442–2450, Oct. 2002.

[53] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1948.

[54] U. Maurer, "Unconditionally secure key agreement and the intrinsic conditional information," vol. 45, pp. 499–514, Mar. 1999.

[55] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography part i: Secret sharing," vol. 39, pp. 1121–1132, July 1993.

[56] M. Block, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," vol. 54, no. 6, pp. 2515–2534, 2008.

[57] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," vol. 41, pp. 1915–1923, Nov. 1995.

[58] L. H. Ozarow and A. D. Wyner, "Wire tap channel II," *AT&T Bell Lab. Tech. J.*, vol. 63, pp. 2135–2157, Dec. 1984.

[59] V. Wei, "Generalized hamming weights for linear codes," vol. 37, pp. 1412–1418, Sept. 1991.

[60] U. Wachsmann, Robert F. H. Fischer, and Johannes B. Huber, "Multilevel codes: theoretical concepts and practical design rules," *IEEE Trans. Inf. Theory.*, vol. 45, pp. 1361–1391, 1999.

[61] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Trans. Inf. Theory.*, vol. 28, pp. 55–67, 1982.

[62] H. Hirakawa and S. Imai, "A new multilevel coding method using error-correcting codes," *IEEE Trans. Inf. Theory.*, vol. 23, pp. 371–377, 1977.

[63] P. A. Martin and D. P. Taylor, "On multilevel codes and iterative multistage decoding," *IEEE Trans. Commun.*, vol. 49, pp. 1916–1925, 2001.

[64] J. S. Yedidia, S. C. Draper and Y. Wang, "Multi-stage decoding of ldpc codes," in *IEEE International Symposium on Information Theory*, (Seoul, Korea), pp. 2151–2155, 2009.

[65] A. R. Calderbank, "Multilevel codes and multistage decoding," *IEEE Trans. Commun.*, vol. 37, pp. 222–229, 1989.

[66] H. Taki and T. Ohtsuki, "Low-density parity-check (LDPC) coded MIMO systems with iterative turbo decoding," in *in Proc. Vehicular Technology Conference*, (Tokyo, Japan), May 2004.

[67] M. A. S. Thomas J. Richardson and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inf. Theory.*, vol. 47, pp. 619–637, Feb 2001.

[68] R. M. T. H. Song and J. R. Cruz, "Low density parity check codes for magnetic recording channels," *IEEE Trans. Magnetic*, vol. 36, pp. 2183 – 2186, Sept. 2000.

[69] J. H. Y. Yi and M. H. Lee, "Design of semi-algebraic low-density parity-check (SA-LDPC) codes for multilevel coded modulation," in *Proc. PDCAT*, (Chengdu, China), pp. 931–934, Aug. 2003.

[70] J. Xiao, X. Ma and S. W. McLaughlin, "Quantifying information rate losses with zero-forcing and maximum-likelihood detectors," in *IEEE Intern. Conf. on Acoustic, Speech and Signal Processing*, (Dallas, U.S.), Mar. 2010.

[71] Z. Drezner, "Computation of the multivariate normal integral," *ACM Transactions on Mathematical Software*, vol. 18, pp. 470–480, Dec. 1992.

[72] A. Genz, "Numerical computation of rectangular bivariate and trivariate normal and t probabilities," *Statistics and Computing*, vol. 14, pp. 151–160, 2004.

[73] T. P. Hutchinson, "Comments on the multivariate normal integral," *J. Stat. Comp. and Simulation*, vol. 47, no. 1, pp. 112–114, 1993.

[74] A. Genz, "Numerical computation of multivariate Normal probablities," *J. Comp. Graph Stat.*, vol. 1, no. 11, pp. 141–149, 1992.

[75] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," vol. 24, pp. 339–348, 1978.

[76] M. van Dijk, "on a special class of broadcast channels with confidential messages," vol. 43, pp. 712–714, Mar. 1997.

[77] Y. Liang, H. V. Poor, and S. Shamai, "Secrecy capacity region of fading broadcase channels," in *Proc. IEEE Int. Symp. Information Theory*, (Nice, France), pp. 1291–1295, June 2007.

[78] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Proc. 44th Annu. Allerton Conf. Communications, Control and Computing*, (Monticello, IL), pp. 841–848, Sept. 2006.

[79] U. Maurer, "Secret key agreement by public discussion from common information," vol. 39, pp. 733–742, May 1993.

[80] D. Klinc, J. ha, S. W. McLaughlin, J. Barros, and B. J. Kwak, "LDPC codes for the Gaussian wiretap channel," in *Proc. Information Theory Workshop*, Oct. 2009.

[81] R. Liu, Y. Liang, H. V. Poor, and P. Spasojević, "Secure nested codes for type ii wiretap channels," in *Proc. 2007 IEEE Information Theory Workshop*, (Lake Tahoe, CA), pp. 337–342, Sept. 2007.

[82] J. Muramatsu, "Secret key agreement from correlated source outputs using low density parity check matrices," *IEICE Trans. Fund. Elec. Comm. Comp.*, vol. E89-A, p. 2036C2046, July 2006.

[83] Y. Xin, Z. Wang, and G. B. Giannakis, "Space-time diversity systems based on linear constellation precoding," *IEEE Trans. Wireless Communications*, vol. 2, pp. 294–309, Mar. 2003.

[84] X. Ma and G. B. Giannakis, "Complex field coded MIMO systems: performance, rate, and tradeoffs," *Wireless Communications and Mobile Computing*, pp. 693–717, Nov. 2002.

# VITA

Jiaxi Xiao was born in Zunyi, Guizhou Province, China. She received the B.S. and M.S. degrees in Precision Instrument from the Tsinghua University of China, Beijing, China, in 2003 and 2005, respectively. In 2011, she received the Ph.D. degree in Electrical and Computer Engineering at Georgia Institute of Technology.